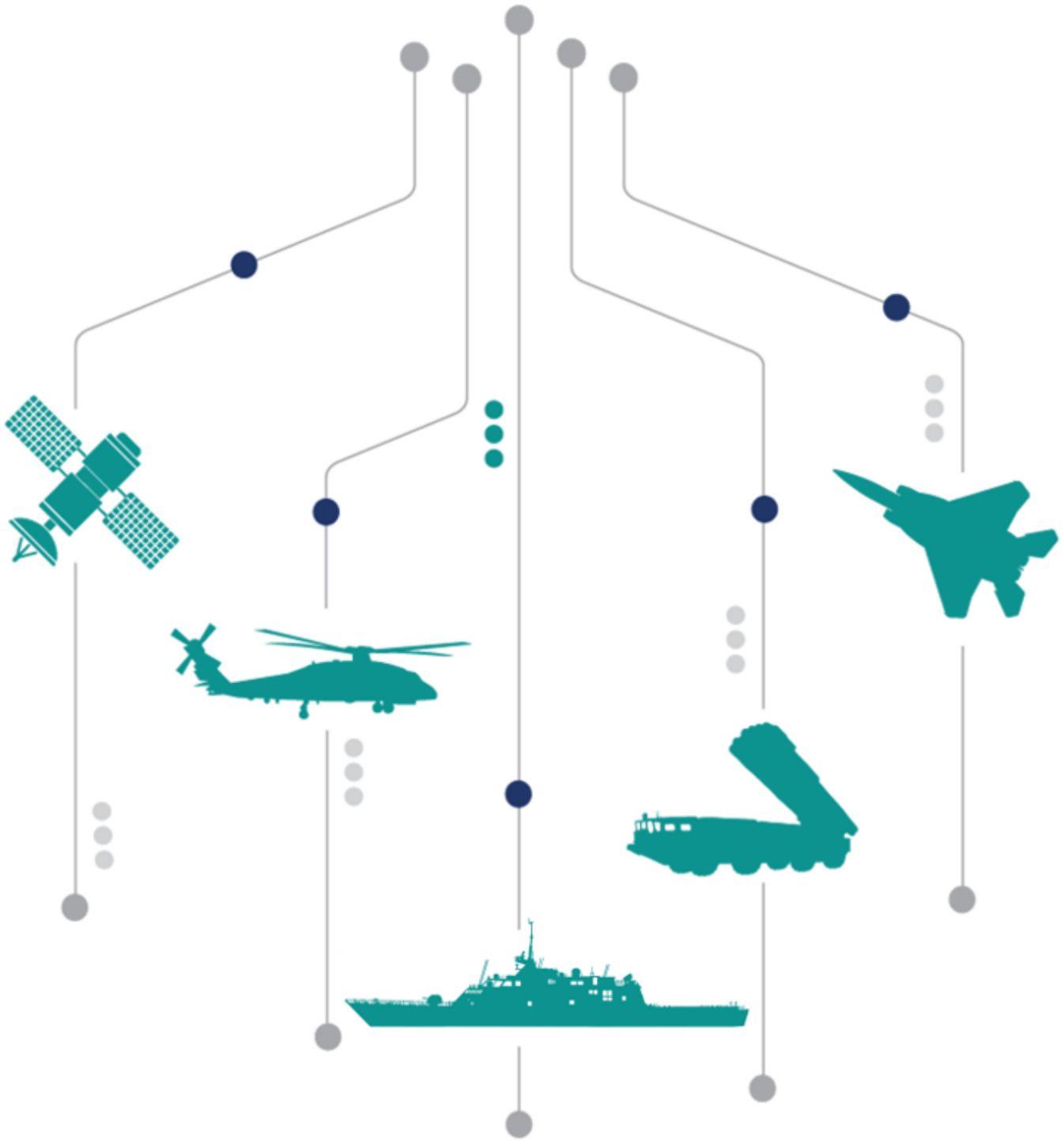


# Cyber Resiliency Scoreboard®



**LOCKHEED MARTIN** 

# Cyber Resiliency Scoreboard® (CRS®)

Lockheed Martin integrates full-spectrum cyber capabilities into everything we deliver to our customers. We introduced the Cyber Resiliency Level® (CRL®) Framework in 2018 as the world's first, standard method to measure the cyber resiliency maturity of a weapon system anywhere in its life cycle. In support of the CRL® Framework, we 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.

## Overview

CRS® is used to identify the maturity level for each of the six CRL® categories: Visibility, Cyber Hygiene, Requirements, Test and Evaluation, Architecture, and Information Sharing (see Figure 1). Each category is split into four levels of increasing maturity: CRL® 1 – Ad-hoc, CRL® 2 – Managed, CRL® 3 – Optimized, and CRL® 4 – Adaptive.

Cyber Resiliency Level®				
Category	Least <span style="float:right">Most</span>			
	CRL® 1	CRL® 2	CRL® 3	CRL® 4
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

Figure 1. Cyber Resiliency Level® Framework V3.01

The CRS® consists of a questionnaire and dashboard displaying qualitative and quantifiable performance metrics used to guide stakeholders in selecting COAs for increased cyber resilience of systems from conception through delivery to retirement. Our innovative CRS® questionnaire is used to capture inputs from subject matter experts (SMEs) about a system's current state of cybersecurity. Our intuitive dashboard then performs data analytics that can be leveraged to assist stakeholders in assessing and measuring CRL® category maturity levels.

## Usage

The CRS® questionnaire is designed to be completed by cyber SMEs. Once the questionnaire is completed, the data is processed, and the results are displayed via the dashboard (Figure 2).

Exceedances		Secondary Watch Items		Criteria Remaining to Reach the To-Be State		Visibility		Cyber Hygiene	
These are the questions where the respondents indicated the program is performing at a level higher than the program's target To-Be CRL® category levels.		These are additional secondary questions that fall within the program's To-Be CRL® category that the program is not currently meeting. While the questions below are not directly used in the CRL® category measurement calculation, the program should review these watch items and discuss potential courses of action.		These are the questions that the program needs to address in order to achieve the specified To-Be state.		Question	CRL® Alignment	Question	CRL® Alignment
Question	CRL® Alignment	Question	CRL® Alignment	Question	CRL® Alignment	Question	CRL® Alignment	Question	CRL® Alignment
VIS-07P	4	VIS-16	3	VIS-04P	3	REQ-04P	3		
CBH-05P	3	CBH-15	2	VIS-05P	3				
CBH-06P	3	REQ-09	3						
CBH-07P	3	REQ-10	3						
CBH-08P	3	REQ-11	3						
CBH-18	4	ARCH-12	3						
REQ-13	4	ARCH-13	3						
T&E-10	3	IS-15	3						
T&E-12	3	IS-16	3						
IS-08P	4								
IS-09P	4								
IS-17	4								

Figure 2. Cyber Resiliency Scoreboard® Dashboard

The dashboard metrics provide a CRL® category "as-is" and/or "to-be" measurement which is displayed using a radar chart (Figure 3).

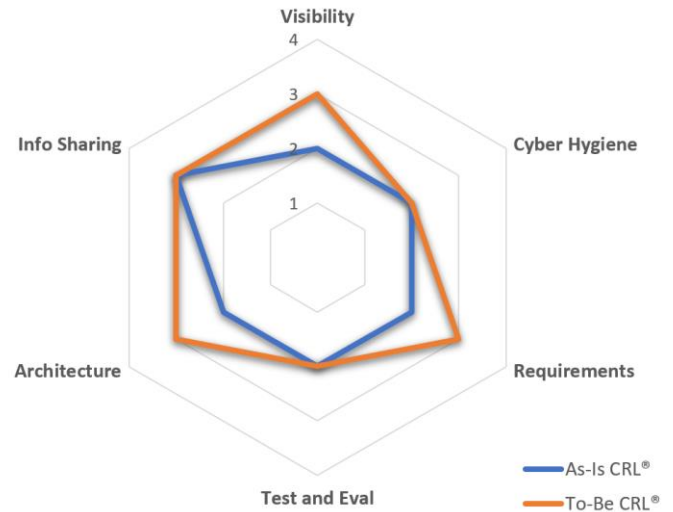


Figure 3. Cyber Resiliency Scoreboard® Radar Chart

CRS® is easily adaptable and has been successfully applied to numerous programs across each of our business areas. 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 how CRS® can enable you to assess and improve your program's cyber resiliency, visit [lockheedmartin.com/crs](https://lockheedmartin.com/crs) and contact us at [cyber.resiliency@lmco.com](mailto:cyber.resiliency@lmco.com).

<sup>1</sup> Additional information on the Lockheed Martin CRL® framework categories and maturity levels is available at [lockheedmartin.com/crl](https://lockheedmartin.com/crl)