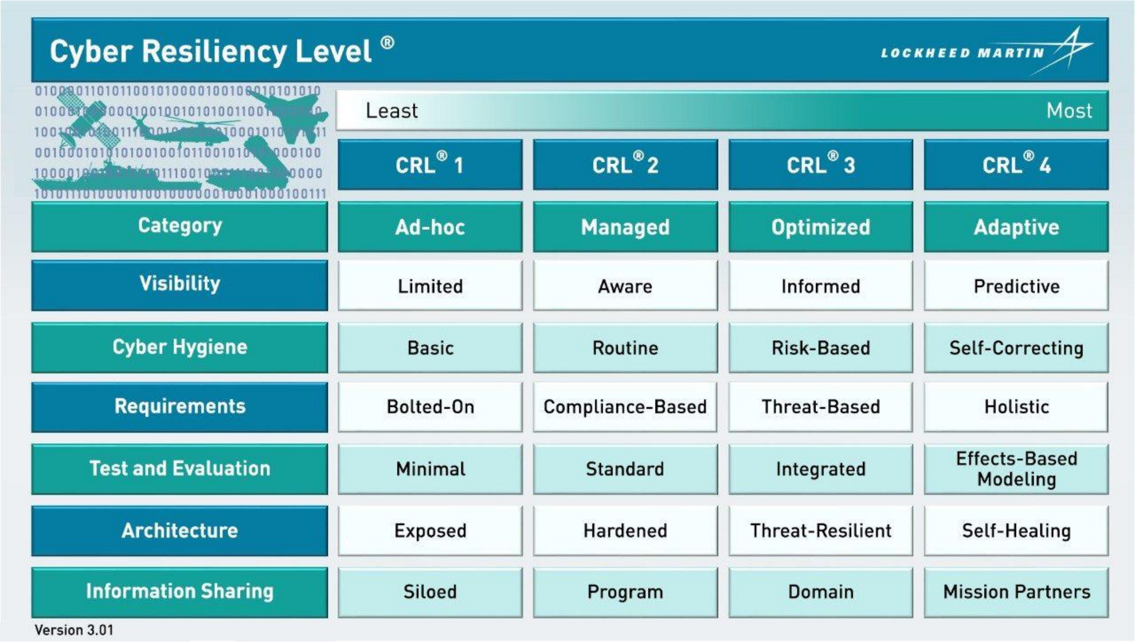
The Lockheed Martin Cyber Resiliency Level® (CRL®) Framework is a standard way to measure the cyber resiliency maturity of weapon, mission, and/or training systems.

Cyber resiliency *is the ability to anticipate, withstand, recover from, and adapt to changing conditions in order to maintain the functions necessary for mission effective capability*[1,2,3]*.*

Overview

CRL® leverages common risk- and engineering-based approaches to measure resiliency across six categories (see Figure 1). These six categories form the major recurring concerns of the United States (U.S.) Department of Defense and were pulled from across their strategy, policies, practices, testimonies, and conference proceedings. An overview of each category is provided below:

1. **Visibility –** Ability to sense, collect, and fuse data to inform defense and response
2. **Cyber Hygiene –** Ability to efficiently assess and maintain the effectiveness of cyber controls
3. **Requirements –** Ability to identify, analyze, and define specifications commensurate with mission importance, risk, and the operational environment
4. **Test and Evaluation –** Ability to measure the effectiveness of controls against mission objectives
5. **Architecture –** Ability to maintain capability against cyber attacks
6. **Information Sharing –** Ability to share timely cyber threat information and defensive measures to improve cyber defensive posture



Cyber Resiliency Level ®

LOCKHEED MARTIN

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 3.01

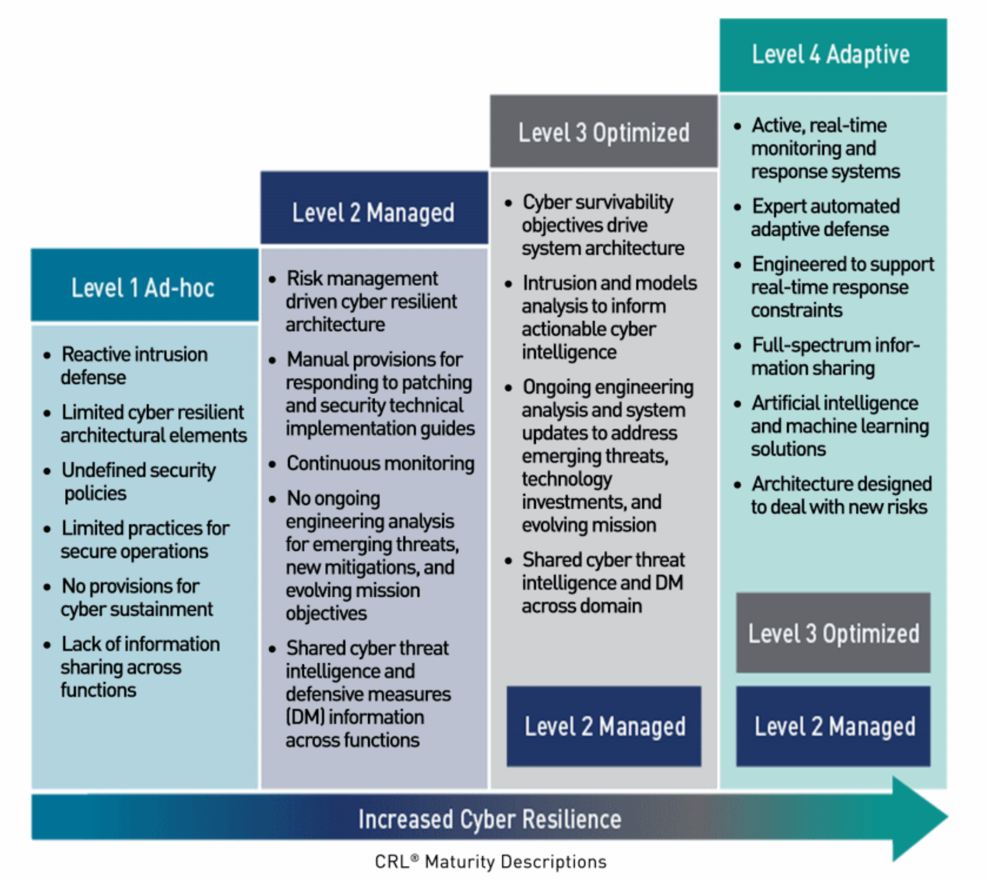
Figure 1. Cyber Resiliency Level® Framework V3.01

Each category is split into four levels of increasing maturity: CRL® 1 – Ad-hoc, CRL® 2 – Managed, CRL® 3 – Optimized, and CRL® 4 – Adaptive (see Figure 2).

[1] Joint Chiefs of Staff. (2018). *Joint Publication 3-14: Space Operations.*

[2] U.S. Air Force. (2017). Cyber Resiliency Office for Weapon Systems briefing.

[3] National Institute of Standards and Technology. (2019). *SP 800-160V2: Developing Cyber Resilient Systems - A Systems Security Engineering Approach.*



Level 1 Ad-hoc

- Reactive intrusion defense
- Limited cyber resilient architectural elements
- Undefined security policies
- Limited practices for secure operations
- No provisions for cyber sustainment
- Lack of information sharing across functions

Level 2 Managed

- Risk management driven cyber resilient architecture
- Manual provisions for responding to patching and security technical implementation guides
- Continuous monitoring
- No ongoing engineering analysis for emerging threats, new mitigations, and evolving mission objectives
- Shared cyber threat intelligence and defensive measures (DM) information across functions

Level 3 Optimized

- Cyber survivability objectives drive system architecture
- Intrusion and models analysis to inform actionable cyber intelligence
- Ongoing engineering analysis and system updates to address emerging threats, technology investments, and evolving mission
- Shared cyber threat intelligence and DM across domain

Level 2 Managed

Level 4 Adaptive

- Active, real-time monitoring and response systems
- Expert automated adaptive defense
- Engineered to support real-time response constraints
- Full-spectrum information sharing
- Artificial intelligence and machine learning solutions
- Architecture designed to deal with new risks

Level 3 Optimized

Level 2 Managed

Increased Cyber Resilience

CRL® Maturity Descriptions

Figure 2. CRL® Maturity Descriptions

Usage

CRL® can be used in any phase of the acquisition life cycle, concept to sunset, and—depending on the scope of the measurement—in any environment, such as development, manufacturing, operations, and supply chain. The structured set of methodologies, processes, and practices can be used to assist stakeholders in prioritizing risks and selecting courses of action for maximum effect against cyber attacks; and, provides stakeholders with an understanding of cyber investments necessary for increased cyber resilience. The CRL® embraces the following four steps[4]:

1. Identify level of cyber resiliency that currently exists and/or is planned.
2. Assess cyber risk.
3. Identify relationships between cyber investments and amount of increased resilience to attack.
4. Prioritize recommendations for cyber investment.

For more information on usage, refer to the whitepaper “Lockheed Martin Cyber Resiliency Level® (CRL®) Framework v3.01 for Weapon, Mission, and Training Systems.”

For additional information:

Lockheed Martin Corporation
Contact: cyber.resiliency@lmco.com
www.lockheedmartin.com/crl

[4] Defense Science Board (DSB). (2016). DSB Task Force Report on Cyber Defense Management.