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 adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.*[1]

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.

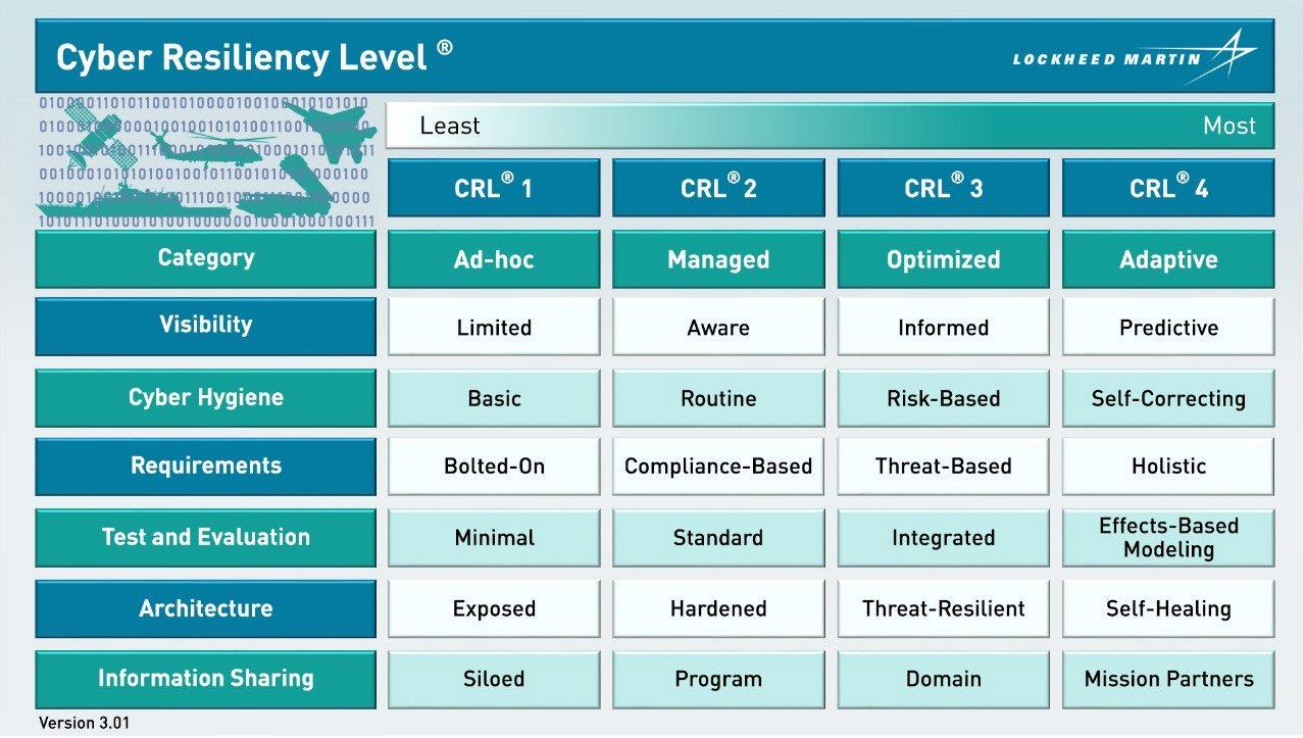

Figure 1. Cyber Resiliency Level® Framework V3.01

[1] National Institute of Standards and Technology. (2021). *NIST Special Publication 800-160, Volume 2. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*

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).

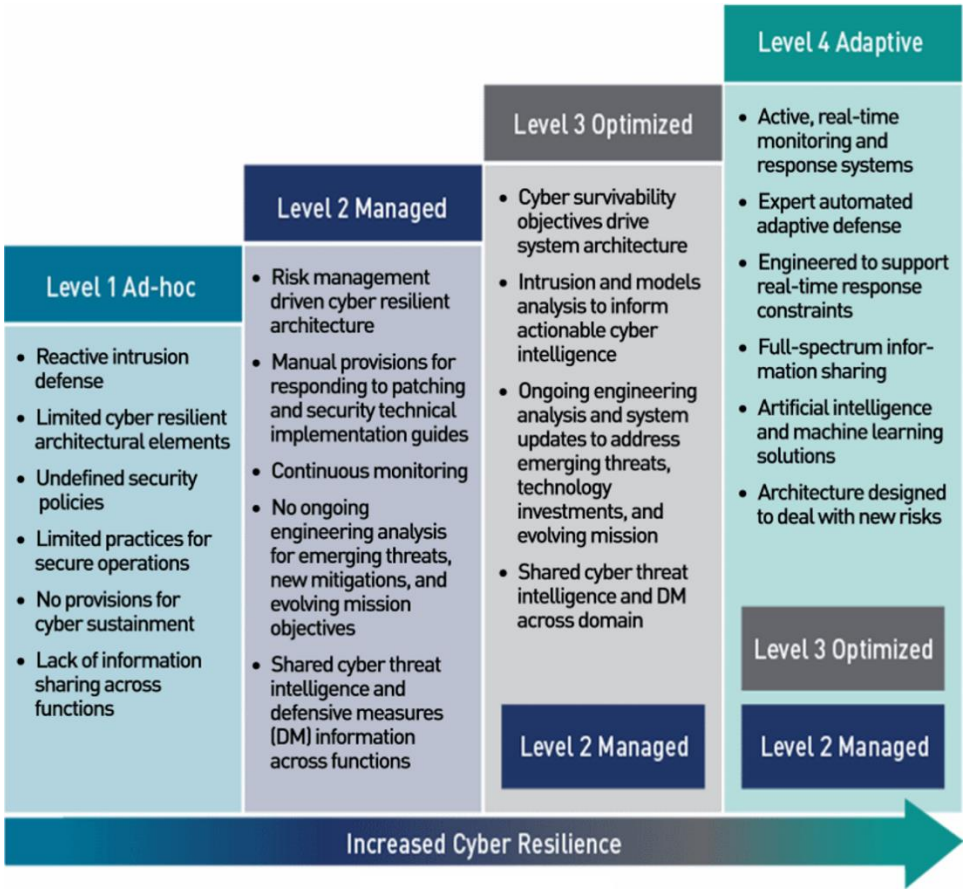

Figure 2. CRL® Maturity Descriptions

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[2]:

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.

To learn more about how CRL® can enable you to assess and improve your cyber resiliency, visit https://www.lockheedmartin.com/crl and contact us at cyber.resiliency@lmco.com.

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