CR-CMM Advisory Board Meeting Summary – November 2025

The Cyber Resilience Capability Maturity Model (CR-CMM) Advisory Board convened in November 2025 to review the Threat-Informed Defense and Defensible Architecture capability areas. See below the summary of the topics discussed and action items.

From	Topic	CR-CMM Area	Next Steps
Perry Young	Need for an underlying attack / asset / system design model that ties Secure-by-Design to CR-CMM	Enablers (Security Architecture, Threat Modeling)	1) Define the model explicitly in CR-CMM; add a section explaining the integration of asset → threat → design layers 2) Add training guidance + asset-centric threat modeling guidance; clarify in CR-CMM narrative
Perry Young	How to incorporate PASTA, STRIDE, ATLAS, ATT&CK, etc. (used together, not in isolation)	Supporting Materials	3) Add guidance for threat modeling under Enablers; define maturity progression. Create a mapping table of methods → CR-CMM goals; describe how to use methods in combination
Carlos Recalde	Asset evaluation must include context: business, threat, design. Need to shift mental model from legacy thinking → resilience model (MVB,	Enablers (Asset Management, Risk Drivers)	4) Add guidance to include BIA, criticality, and context must evolve beyond traditional and explicitly require contextual evaluation.

	high-value targets)		
Carlos Recalde and Itay Mesholam	Dependency mapping needs to go beyond CMDB. BIA should be mentioned in the Enablers and expand beyond IT BIA.	Capabilities (Criticality Analysis) + Enablers (Asset Management)	5) Add dependency-mapping maturity criteria, include supply-chain dependencies. 6) BIA should be Operational Resilience BIA, not just IT BIA. Rewrite BIA section; integrate people, process, tech, suppliers.
Perry Young	Need to map the 4 Goals of Cyber Resilience to CSF phases + governance	Supporting Materials	7) Create a crosswalk: CR-CMM Goals ↔ CSF Functions ↔ NIST 800-160 ↔ Governance 8) Include guidance on CWE references in threat modeling & architecture sections (beyond what's vulnerable)

Closing notes

1. The Advisory Board continues to gather to review CR-CMM Capabilities.
2. Please refer to the October Advisory Board meeting notes for more details on overall strategy for the CR-CMM.

Agreed Initiatives (2026)

a) Launch of a mapping initiative across all CR-CMM practices to enhance interoperability and credibility with frameworks (NIST, ISO etc).
b) Update and expansion of FAQs to emphasize resilience as a strategic, top-down initiative.
c) Integration of a feedback and survey mechanism on the CR-CMM website to better understand user motivations and engagement.
d) Development of a CR-CMM roadmap for 2026, focusing on practical adoption, evidence-based assessment, and risk quantification capabilities.