EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

- Supply chain risks have continued to grow dramatically as a result of expanded outsourcing of technology and infrastructure, as well as the scope and complexity of the threat landscape. Managing these risks has become an organizational imperative as customers and stockholders have registered their concern over failures that have affected millions of individuals.
- The complexities and challenges of external dependencies management (EDM) require the use of systematic and comprehensive methods that provide simple, actionable recommendations.
- The DHS Cyber Security Evaluation Program offers an External Dependencies Management Assessment (EDM Assessment). The EDM Assessment is a no-cost, voluntary, non-technical assessment to evaluate and communicate the EDM capability of critical infrastructure organizations.
- The EDM Assessment is part of a portfolio of cyber security assessment products to assist the owners and operators of critical infrastructure. More information can be obtained by emailing the DHS Cyber Security Evaluation Program at CSE@hq.dhs.gov.

The EDM Assessment draws on risk and cybersecurity management techniques developed over the last twelve years by leading private and public organizations. The approach leverages a resilience management methodology developed through a collaborative private-public initiative at Carnegie Mellon University. These methods have been further refined and informed by hundreds of assessments and implementations.

OVERVIEW

The EDM Assessment addresses an increasingly common challenge; how to ensure the security and resilience of your organization's critical services when many of their supporting assets – technology, people, facilities, and information - are provided by third parties. The array of these suppliers is vast and includes contracted vendors as well as infrastructure and shared or public services, (e.g., power, water, fire, police, emergency operations, and road and air transportation).

The EDM Assessment evolved from the DHS Cyber Resilience Review (CRR), and borrows the CRR's structure and assessment approach. Both assessment tools are based on the CERT Resilience Management Model (RMM) [http://www.cert.org/resilience/rmm.html], a capability maturity model for managing operational resilience, developed by the CERT Division of Carnegie Mellon University's Software Engineering Institute.

The purpose of the EDM Assessment is to develop your organization's understanding of how well it manages the risks arising from external dependencies, specifically dependencies on the information and communication technology (ICT) service supply chain. The ICT service supply chain consists of outside parties that operate, provide, or maintain information and communications technology for the organization. Common examples include externally provided web and data hosting, telecommunications services, and data centers.

The EDM Assessment evaluates the organization's risk management when forming relationships with external entities, ongoing management of third party relationships, and the ability to sustain services when external entities fail to meet the terms of service or are otherwise disrupted.

The EDM Assessment focuses on services and assets. It uses the relationships between high value services and assets – people, technology, facilities, and information – to scope and organize the assessment. Together these concepts clarify how well an organization manages the risks it incurs from using external entities to support essential services or products.

To provide the organization with an understandable and useful structure for the evaluation, the EDM Assessment is divided into three distinct areas (domains):

1. **RELATIONSHIP FORMATION –** how the organization considers third party risks, selects external entities, and forms relationships with them so that risk is managed from the start

2. **RELATIONSHIP MANAGEMENT AND GOVERNANCE –** how the organization manages ongoing relationships with external entities to support and strengthen its critical services at a managed level of risk and cost

3. **SERVICE PROTECTION AND SUSTAINMENT –** how the organization plans for, anticipates, and manages disruption or incidents related to the external entities it depends on

The EDM Assessment seeks participation from the organization's staff in the business, operations, procurement, legal, security, and information technology functions. Their representatives may include personnel with the following roles and responsibilities:

- **IT policy & procedures** (e.g., Chief Information Security Officer)
- **Business operations** (e.g., operations manager)
- **Procurement and vendor management**
- **IT security planning & management** (e.g., Director of Information Technology)
- **IT infrastructure** (e.g., network/system administrator)
- **IT operations** (e.g., configuration/change manager)**Business continuity & disaster recovery planning** (e.g., BC/DR manager)
- **Risk analysis** (e.g., enterprise/operations risk manager)
- **Legal** (legal support to critical service)

EDM ASSESSMENT PROCESS

The EDM Assessment is a four hour facilitated event held at a location of the organization's choosing. The on-site facilitated session involves DHS representatives trained to use the assessment. The organization can expect a variety of benefits from conducting an EDM Assessment:

- a clear, comprehensive way to understand the organization's third party risk management capabilities and express them to its stakeholders

- a better understanding of the organization's cybersecurity posture as it relates to external dependencies

- an opportunity for participants from different parts of the organization to discuss issues relating to vendors and reliance on third parties

- an identification of improvement areas for managing third parties that support the organization

The EDM Assessment generates a report as a final product. The report contains each of the assessment's questions and answers, a convenient mapping graphic that displays capability in the assessed areas, and relevant options for consideration. The options for consideration refer to recognized standards and best practices, including references to the CERT RMM, that are intended to help the organization improve its EDM capability.

The EDM Assessment report is created exclusively for the organization's internal use. DHS uses information collected during an EDM Assessment for anonymized data analytics only. Anonymized data analytics and reporting are intended to benefit critical infrastructure owners and operators in the United States. Any information discussed is protected under the DHS Protected Critical Infrastructure Information (PCII) Program [www.dhs.gov/pcii].

HOW DO I REQUEST A REVIEW?

To schedule a facilitated EDM Assessment or to request additional information please email the Cyber Security Evaluation program at CSE@hq.dhs.gov.