Homeland Security

Stakeholder Engagement
and Cyber Infrastructure Resilience

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 stakeholders have registered their concern over failures that have affected millions of individuals.
- To address these challenges the Department of Homeland Security (DHS) Office of Cybersecurity and Communications (CS&C) has developed a systematic and comprehensive assessment tool, the External Dependencies Management Assessment (EDM Assessment). The assessment helps to evaluate and communicate the capability of critical infrastructure organizations to manage external dependencies, specifically information and communication technology (ICT) supply chain risk.
- The EDM Assessment is a no-cost, voluntary, non-technical assessment which is part of a portfolio of tools and methods to assist the owners and operators of critical infrastructure. More information can be obtained by emailing the DHS Cyber Security Advisor program at cyberadvisor@hq.dhs.gov .

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. These dependencies can vary and include contracted vendors as well as infrastructure (e.g., power, water and telecommunications) and government services (e.g., fire, police and emergency operations).

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 Carnegie Mellon University CERT Resilience Management Model, developed over the last twelve years by leading private and public organizations. These techniques have been further refined and informed by hundreds of assessments and implementations.

The goals of the EDM Assessment are:

- To assess the activities and practices utilized by an organization to manage risks arising from external dependencies.
- To provide an objective review of capabilities in the assessed areas, and recommendations that offer a roadmap for improvement based on industry leading practices.

The purpose of the EDM Assessment is to provide critical infrastructure organizations an understanding of how they manage risks arising from external dependencies, specifically dependencies on the ICT service supply chain. The ICT service supply chain consists of outside parties that operate, provide, or support information and communications technology for the organization. Common examples include externally provided web and data hosting, telecommunications services, and data centers, as well as any service that depends on the secure use of ICT.

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 an organization manages the risks it incurs from using external entities to support essential services or products.

The External Dependencies Management (EDM) Assessment may be used by itself as an aid to manage external dependencies, or as the first step in an improvement effort. It can also be used in conjunction with DHS's External Dependencies Management *Method* which provides a rigorous, repeatable way to identify and manage specific suppliers or other external entities that the organization depends on to support its mission.

EDM Assessment overview continued:

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 external entities

The EDM Assessment seeks participation from the organization's staff in business and operations areas. Their representatives may include personnel with the following roles and responsibilities:

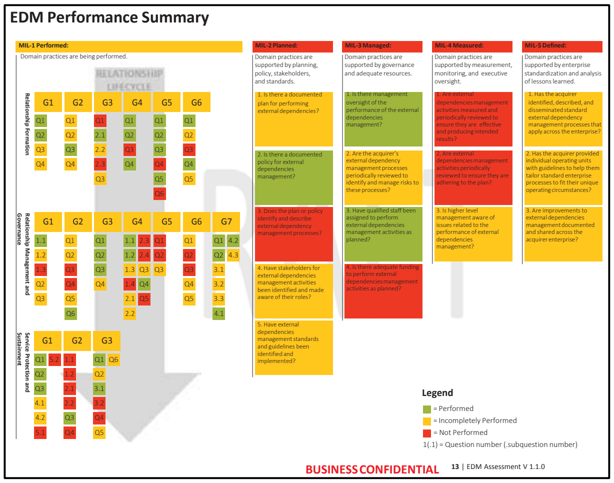
- **IT security planning & management** (e.g., information technology managers)
- **Risk analysis** (e.g., enterprise/operations risk managers)
- **IT policy & procedures** (e.g., Chief Information Security Officer and managers)
- **Procurement and vendor management** (e.g., contracts and legal support managers)
- **IT infrastructure** (e.g., network/system administrator)
- **IT operations** (e.g., configuration/change managers)
- **Business continuity & disaster recovery planning** (e.g., BC/DR manager)
- **Business operations (e.g., operations managers)**
- **Legal** (legal support to a 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 comprehensive report that describes the organization's third party risk management practices and capabilities for its stakeholders
- a better understanding of the organization's cybersecurity posture relating to external dependencies
- an opportunity for participants from different parts of the organization to discuss issues relating to vendors and reliance on external entities
- an identification of improvement areas for managing third parties that support the organization

The EDM Assessment 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 the CERT-RMM, NIST standards, and the NIST Cybersecurity Framework. These are intended to help the organization improve its EDM capability.



EDM Performance Summary

MIL-1 Performed:

Domain practices are being performed.

RELATIONSHIP LIFECYCLE
Relationship Formation
G1 Q1 Q2 Q3 Q4
G2 Q1 Q2 Q3 Q4
G3 Q1 2.1 2.2 2.3 Q3
G4 Q1 Q2 Q3 Q4
G5 Q1 Q2 Q3 Q4 Q5 Q6
G6 Q1 Q2 Q3 Q4 Q5
Relationship Management and Governance
G1 1.1 1.2 1.3 Q2 Q3
G2 Q1 Q2 Q3 Q4 Q5 Q6
G3 Q1 Q2 Q3 Q4
G4 1.1 1.2 1.3 1.4 2.1 2.2 2.3 2.4 Q3 Q4 Q5
G5 Q1 Q2 Q3
G6 Q1 Q2 Q3 Q4 Q5
G7 Q1 Q2 3.1 3.2 3.3 4.1 4.2 4.3
Service Protection and Sustainment
G1 Q1 Q2 Q3 4.1 4.2 5.1 5.2
G2 1.1 1.2 2.1 2.2 Q3 Q4
G3 Q1 Q2 3.1 3.2 Q4 Q5 Q6

MIL-2 Planned:

Domain practices are supported by planning, policy, stakeholders, and standards.

1. Is there a documented plan for performing external dependencies?
2. Is there a documented policy for external dependencies management?
3. Does the plan or policy identify and describe external dependency management processes?
4. Have stakeholders for external dependencies management activities been identified and made aware of their roles?
5. Have external dependencies management standards and guidelines been identified and implemented?

MIL-3 Managed:

Domain practices are supported by governance and adequate resources.

1. Is there management oversight of the performance of the external dependencies management?
2. Are the acquirer's external dependency management processes periodically reviewed to identify and manage risks to these processes?
3. Have qualified staff been assigned to perform external dependencies management activities as planned?
4. Is there adequate funding to perform external dependencies management activities as planned?

MIL-4 Measured:

Domain practices are supported by measurement, monitoring, and executive oversight.

1. Are external dependencies management activities measured and periodically reviewed to ensure they are effective and producing intended results?
2. Are external dependencies management activities periodically reviewed to ensure they are adhering to the plan?
3. Is higher level management aware of issues related to the performance of external dependencies management?

MIL-5 Defined:

Domain practices are supported by enterprise standardization and analysis of lessons learned.

1. Has the acquirer identified, described, and disseminated standard external dependency management processes that apply across the enterprise?
2. Has the acquirer provided individual operating units with guidelines to help them tailor standard enterprise processes to fit their unique operating circumstances?
3. Are improvements to external dependencies management documented and shared across the acquirer enterprise?

Legend

🟩 = Performed

🟨 = Incompletely Performed

🟥 = Not Performed

1(.1) = Question number (.subquestion number)

BUSINESS CONFIDENTIAL 13 | EDM Assessment V 1.1.0

DATA PRIVACY AND SCHEDULING

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 and reporting only. Assessment information is protected under the DHS Protected Critical Infrastructure Information (PCII) Program www.dhs.gov/pcii .

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