Methods and Tools for External Dependencies Management

Ross Gaiser – Department of Homeland Security
John Haller – Software Engineering Institute

January 15, 2015

Notices

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This work was created with the funding and support of the U.S. Department of Homeland Security under the Federal Government Contract Number FA8721-05-C-0003 between the U.S. Department of Defense and Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark of Carnegie Mellon University

Objectives and Approach

Objective: To help critical infrastructure organizations in the United States improve their management of external dependencies (supply chain).

Two main areas of work:

- External Dependency Management Assessment
- Dependency Analysis Method

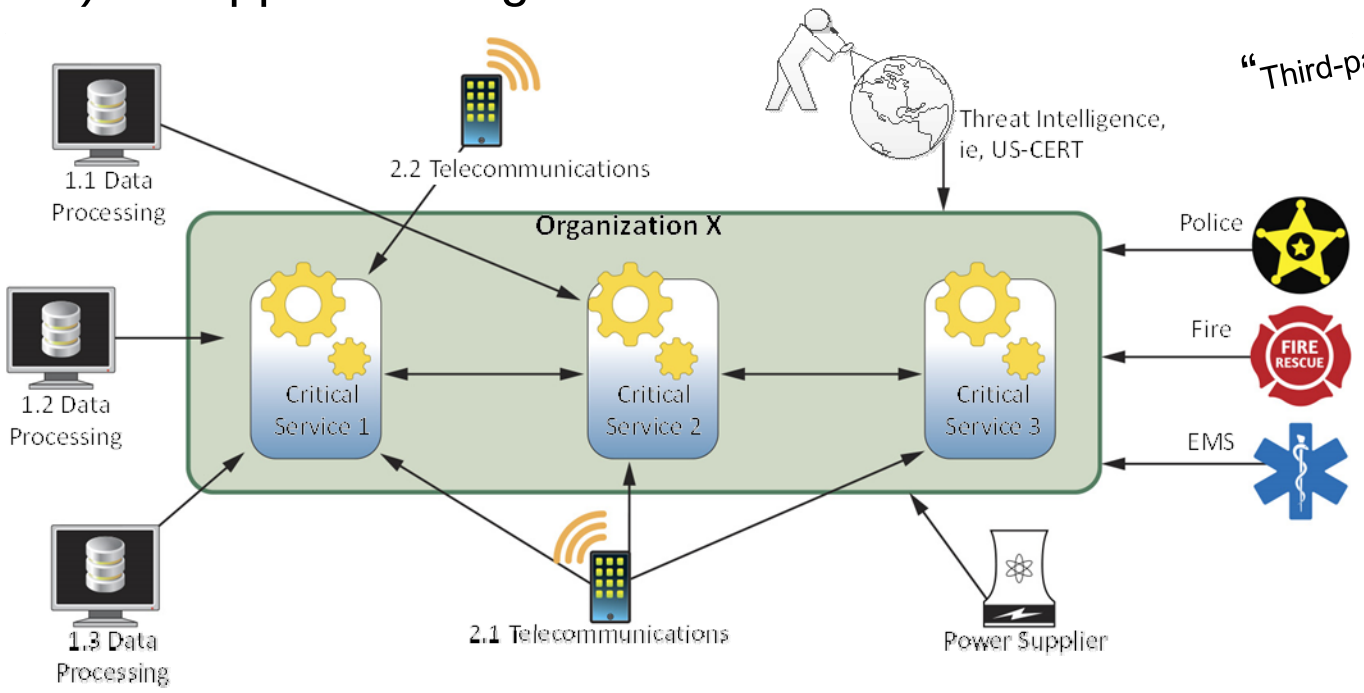
Influenced by and based on:

- CERT Resilience Management Model
- ISO/IEC Standards
- NIST CSF
- DHS Cyber Resilience Review
- ITIL

What do we mean by external dependencies management?

Managing the risk of depending on external entities to support your organization's high value services.

External Dependency Management focuses on external entities that provide, sustain, or operate Information and Communications Technology (ICT) to support the organization.

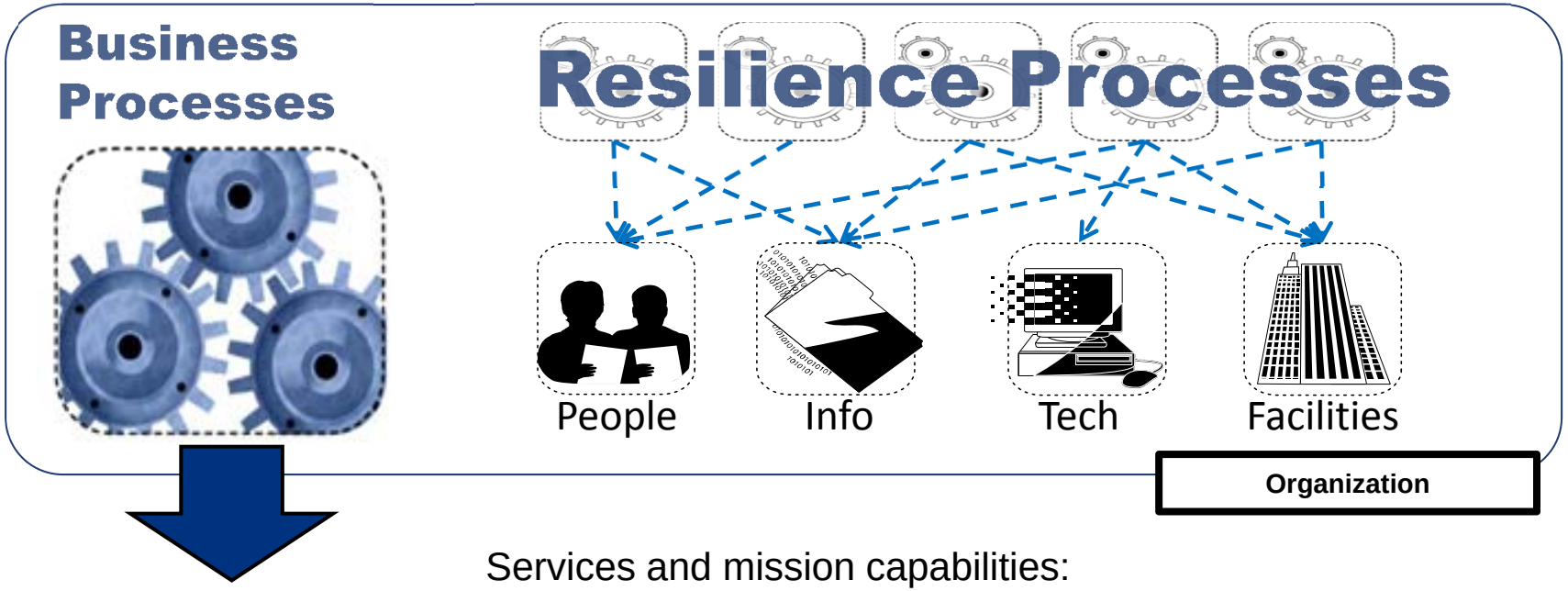


"Third-party risk management"

"Supply chain risk management"

"Vendor management"

Service and asset focus



Services and mission capabilities:

Clearing and settlement

Electricity distribution

ATM network operations

911 Dispatch

Electronic healthcare records

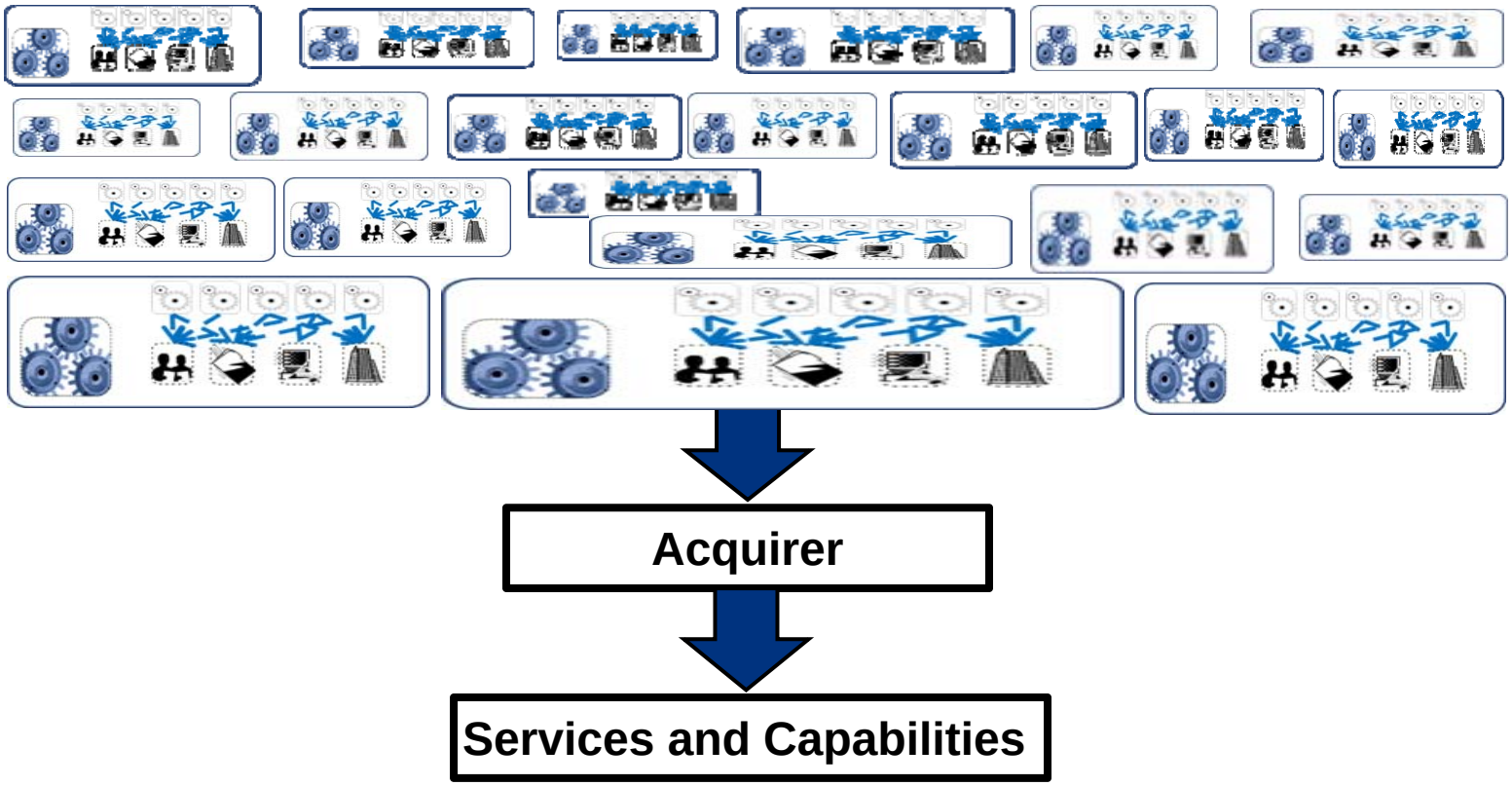
Military transportation

Anti-submarine warfare

Fire support

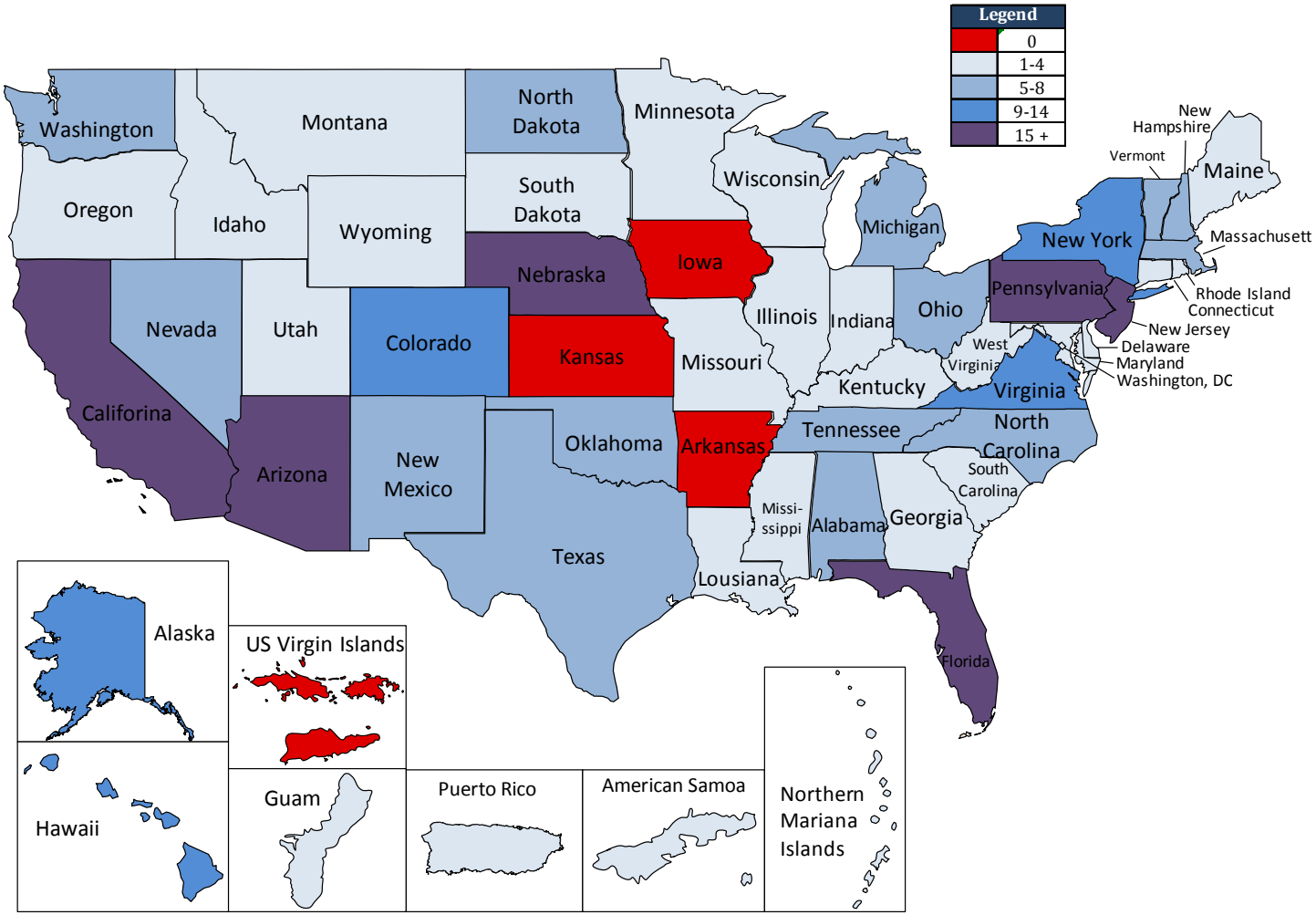
Weapons system acquisition

Supply chain complexity



Essential problems: How to have confidence in resilience processes outside the acquirer's control, and how to manage the risk when you can't.

DHS Cyber Resilience Review influence



Sector	Count
Agriculture and Food	3
Banking and Finance	17
Chemical	0
Commerical Facilities	10
Communications	5
Critical Manufacturing	8
Dams	1
Defense Industrial Base	1
Emergency Services	30
Energy	40
Government Facilities	36
Information Technology	17
National Monuments	1
National Special Events	1
Nuclear Reactors, Waste	0
Postal and shipping	0
Public Health and Healthcare	29
State/LUA	44
Transportation	29
Water	37
Grand Total	**309**

From FY2009– Present (as of 11/25/2014) 309 assessments conducted

Policy across ten CRR domains

DHS External Dependency Management Assessment (EDM Assessment) Overview

An examination of organizational practices and maturity to manage external dependency risk. ***How are we doing, and where can we improve?***

Purpose:

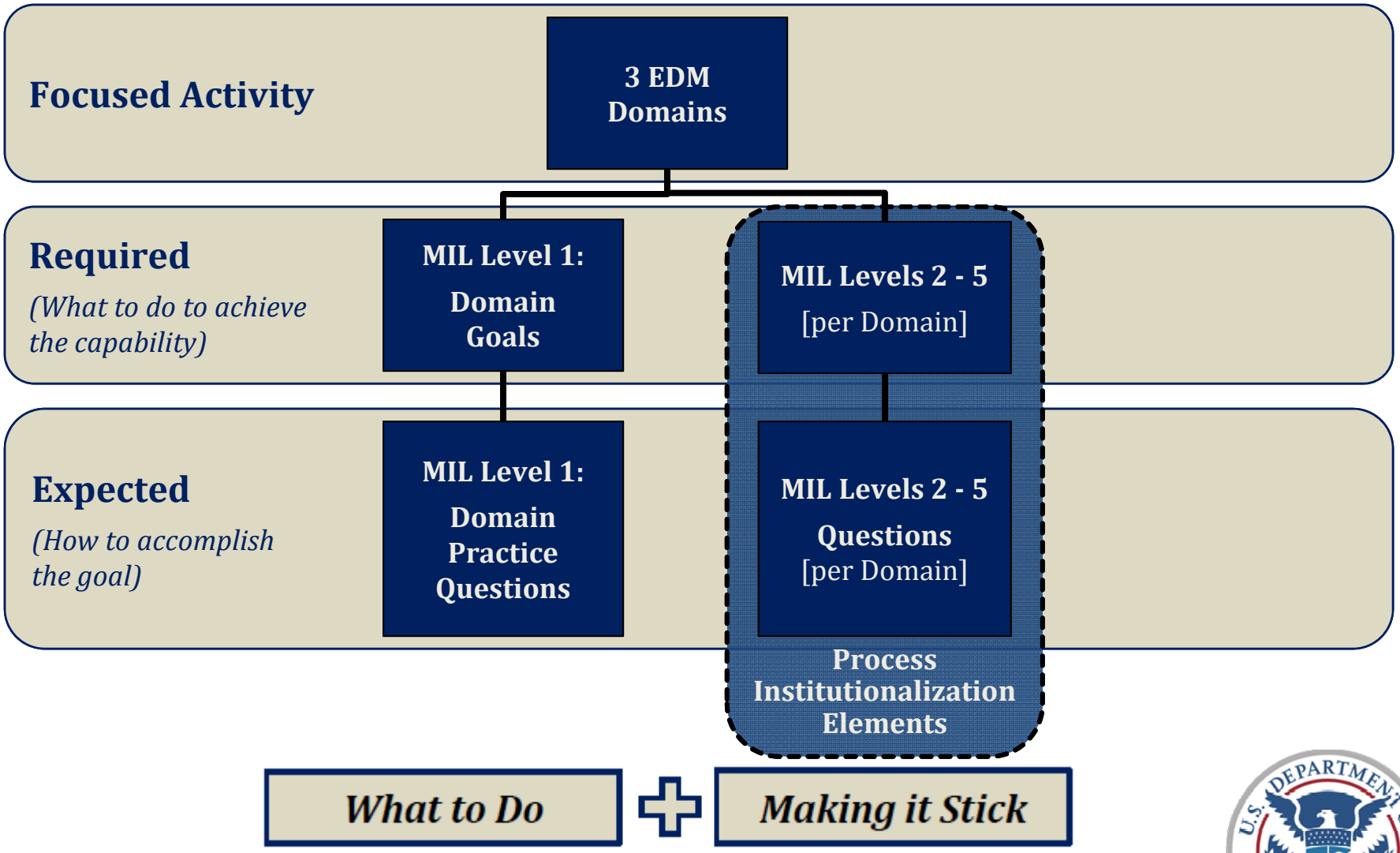
- To assess an acquirer's ability to manage the risks of external dependencies and provide improvement recommendations
- To allow acquiring organizations to compare themselves to peers.

Based on the ***DHS Cyber Resilience Review*** and the ***CERT® Resilience Management Model (CERT® RMM)***, a process improvement model for managing operational resilience

- Developed by Carnegie Mellon University's Software Engineering Institute
- More information: http://www.cert.org/resilience/rmm.html

EDM Assessment - Domains

EDM Assessment - Architecture Overview



EDM Assessment – Sample Questions

Has a plan for selecting and forming relationships with suppliers been established?

Is the ability of suppliers to meet resilience requirements of the critical service considered in the selection process?

Are dependencies on external relationships that are critical to the service(s) identified?

Are vulnerabilities in the organization's external entities that affect the critical service actively discovered?

Are the risks of relying on an external entity to support the critical service identified and managed?

Are service continuity plans tested with external entities?

Maturity indicator levels – sustaining capability

MIL2 – Planned:

Have stakeholders been identified and made aware of their roles?

Is there a documented policy for the domain?

MIL3 – Managed:

Is there management oversight?

Are risks to the process controlled?

MIL4 – Measured

Is the process reviewed for effectiveness?

MIL5 - Defined

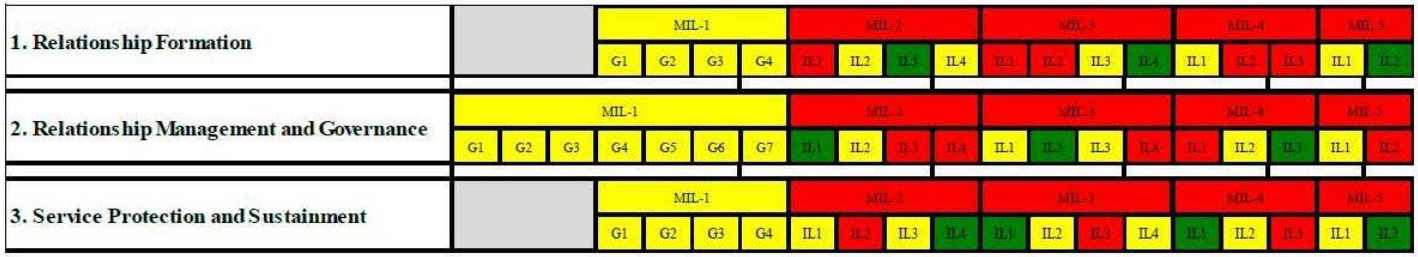
Is there a standard process enterprise wide?

Is there a lessons-learned process?

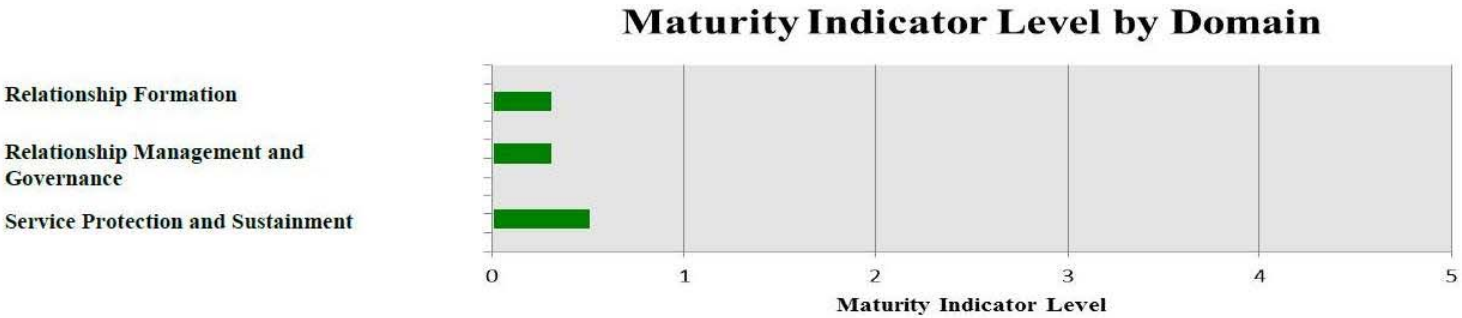
. . .

EDM Assessment Heat Map

Overview of EDM Results



Summary of Results



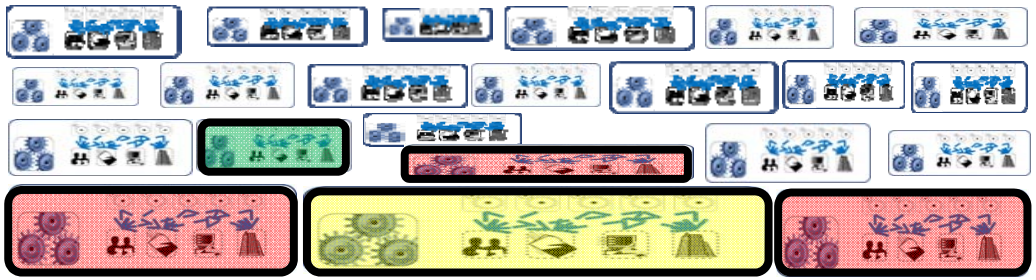
External Dependency Analysis Method (EDA Method) Overview

A method to identify and make decisions about the suppliers that support a specific acquirer service or set of services. ***Whom do we manage and how much?***

Purpose:

- To identify and provide organizational leadership with an *accurate, useful representation* of the organization's critical few suppliers;

- To assess and display the controls and practices applied to a supplier set, so that organizational leadership can make better decisions about their management



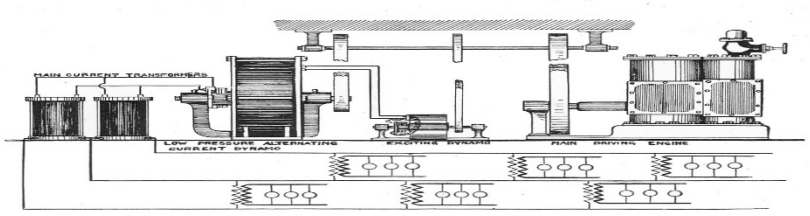
Identifying dependencies: HAVEX attack

Lifecycle and relationship management

Procurement

Deployment

Operation



Periodic software downloads from manufacturer website

Requirement: Integrity of downloaded software installers

Who is managing this relationship?

EDA Method - Process Overview

External entities are identified based on services and relationships with key assets

Entities/suppliers are ranked according to standard impact definitions and aggravating factors

The organization answers fifteen questions per supplier about current practices

The toolset provides a chart of the supplier set comparing supplier criticality to current practices

Standard service impact levels and factors

High service impact:

Disruption to the external entity would result in the critical service failing to meet its requirements and customers or stakeholders experiencing substantial harm.

Medium service impact:

1. A tolerable degradation of the critical service. The service continues to function at its minimum requirements. The disruption may be noticeable to stakeholders but it is an inconvenience. The organization may experience extra costs during the disruption but they are manageable or planned for, or

2. The external entity disruption represents a clear source of risk to the requirements for the critical services or to the assets that support the critical service.

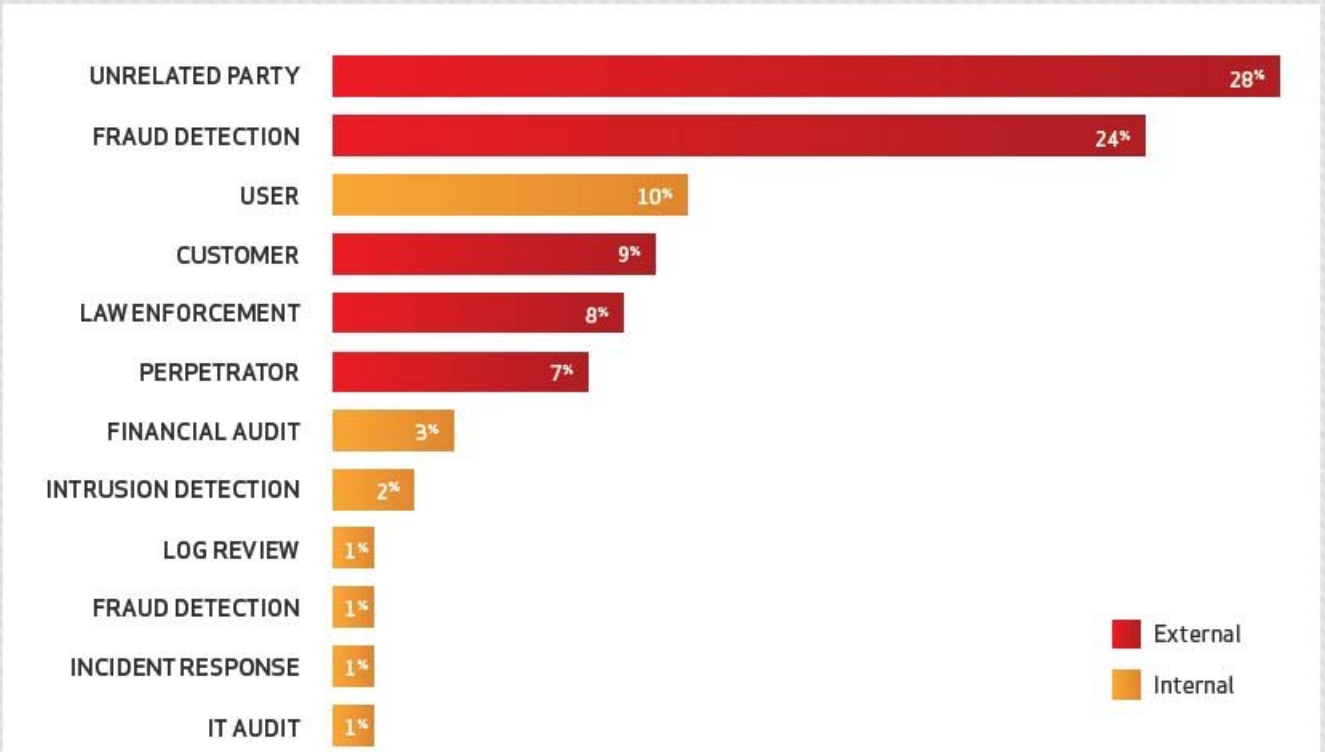
Aggravating factors: Reputational, financial, compliance-related

Management practice implementation

NIST CSF Function	Internal practice	External practice	Cooperative practice
Identify	Does the organization manage the risk of the external entity being a single point of failure?	Does the external entity have a risk management program that is consistent with and supportive of the critical service(s)?	Does the organization periodically review risks and threats with the external entity to maintain both organizations' situational awareness?
Protect	Does the organization document and maintain resilience requirements and control objectives that pertain to the external entity?	Are resilience requirements for the external entity adequately documented in formal agreements with the external entity?	Are the controls at the external entity periodically validated, audited or tested to ensure that they meet organizational requirements?
. . .	. . .	. . .	. . .

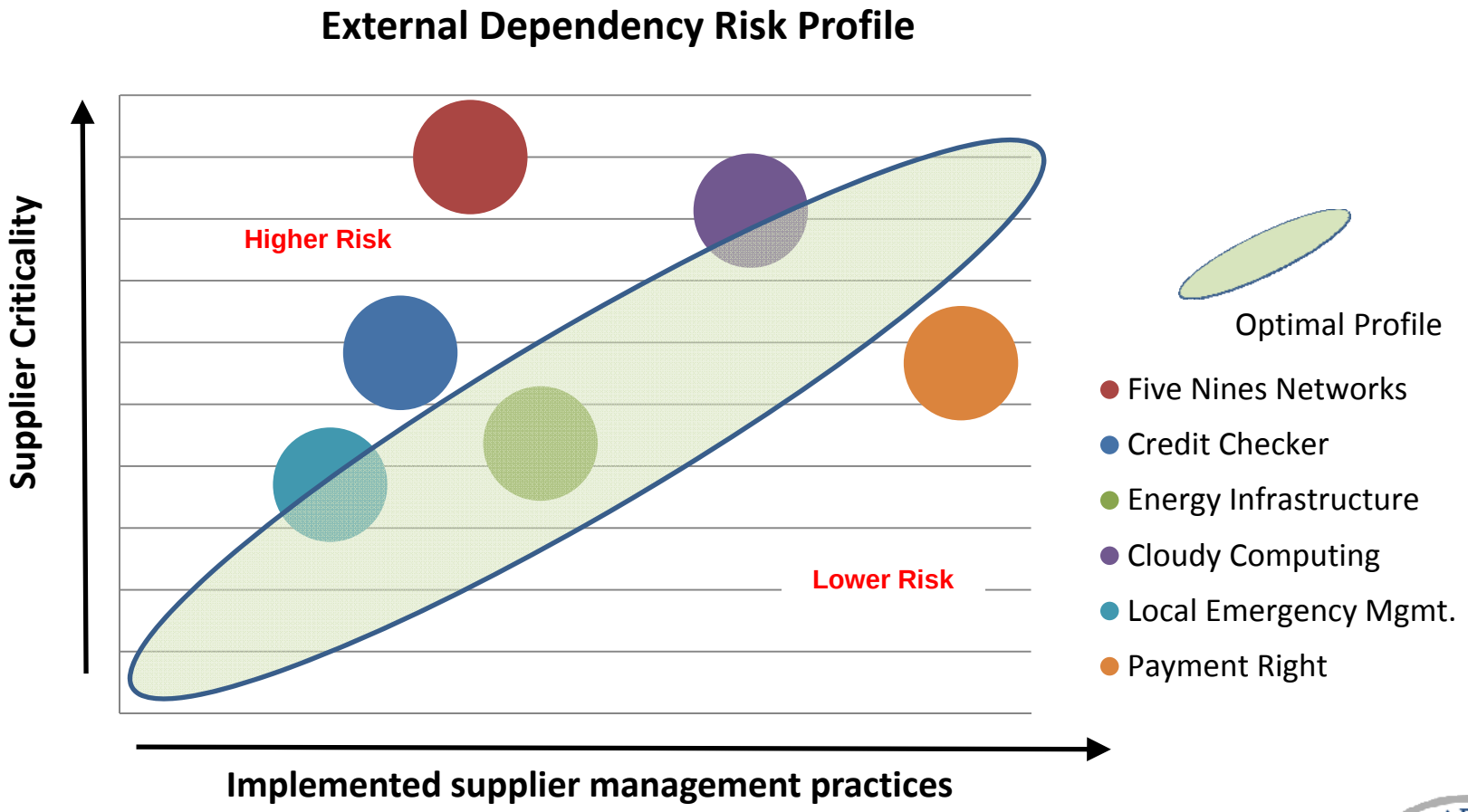
Importance of cooperation and managing the supplier set

Figure 6: Who identifies data breaches



Many organizations devote a disproportionate amount of time and money to detection methods that fall below the 1% mark.

Output


External Dependency Risk Profile
Supplier Criticality
Higher Risk
Lower Risk
Implemented supplier management practices
Optimal Profile
Five Nines Networks
Credit Checker
Energy Infrastructure
Cloudy Computing
Local Emergency Mgmt.
Payment Right

Conclusion: What Is Cyber Resilience?

"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

- Presidential Policy Directive – PPD 21
February 12, 2013

Protect (Security)	**Sustain (Continuity)**
Perform (Capability)	**Repeat (Maturity)**

Conclusion: Why resilience?

Resilience management provides support to *simplify* the management of complex cybersecurity challenges.

Efficiency: not too much and not too little; resilience equilibrium

- balancing risk and cost
- getting the most bang for your buck
- achieving compliance as a by-product of resilience management

Roadmap: what to do to manage cybersecurity; flexibility and scalability

- using an overarching approach - which standard is best
- deciding what versus how to manage cybersecurity risk

Cybersecurity ecosystem: addressing the interconnectedness challenge

- managing dependencies
- addressing internal and external organizational challenges and silos

Questions?

Contact Information Slide Format

Presenter / Point of Contact
Ross Gaiser
DHS – Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR)
Telephone: +1 703-235-5635
Email: Ross.Gaiser@hq.dhs.gov

Presenter / Point of Contact
John Haller
CERT program – SEI
Telephone: +1 412-268-6648
Email: jhaller@cert.org

Web

https://www.dhs.gov/topic/cybersecurity
www.cert.org/resilience