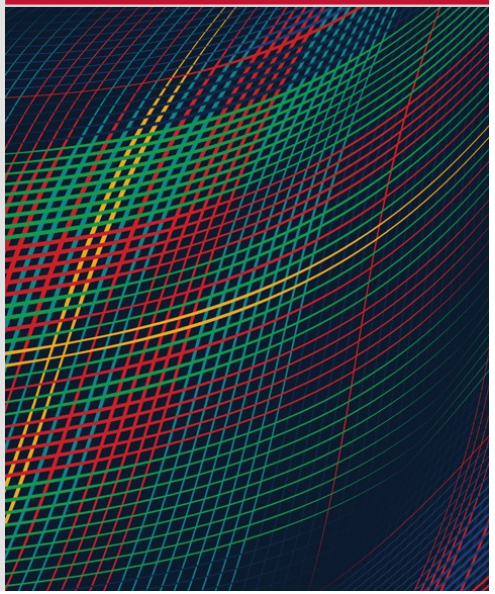
Insider Threat Vulnerability Assessment (ITVA)
Exit Briefing

MONTH 00, 2023

FirstName LastName
Very Smart Researcher

Carnegie Mellon University
Software Engineering Institute



Document Markings

Carnegie Mellon University Software Engineering Institute

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

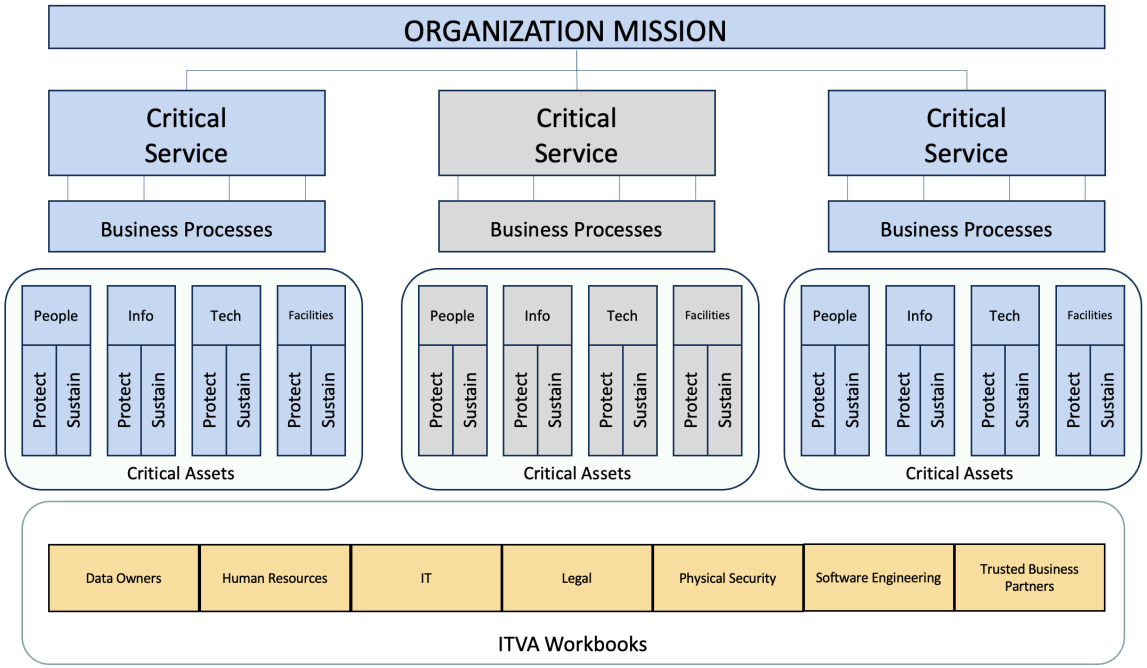
DM23-0882

SEI Insider Risk
ITVA Process Review

Carnegie Mellon University
Software Engineering Institute

Insider Threat Vulnerability Assessment (ITVA) Overview

Carnegie Mellon University Software Engineering Institute



The SEI **measures organizations' preparedness to prevent, detect, and respond to insider threats** to critical assets using its ITVA capability

The ITVA **benchmarks** organizations' technical, physical, and administrative **controls** against the most prevalent **vulnerabilities** from the **CERT Insider Threat Incident Corpus**

The ITVA identifies key capability gaps in the protection of an organization's critical assets from authorized access misuse, and provides recommended mitigation strategies for vulnerabilities to specific assets

Assessment Methodology

Carnegie Mellon University Software Engineering Institute

Assess Scoped Business Processes.

- Conduct interviews with key personnel.
- Review key company artifacts.
- Review data sources used for analysis.
- Review tools.

The ITVA methodology is designed to

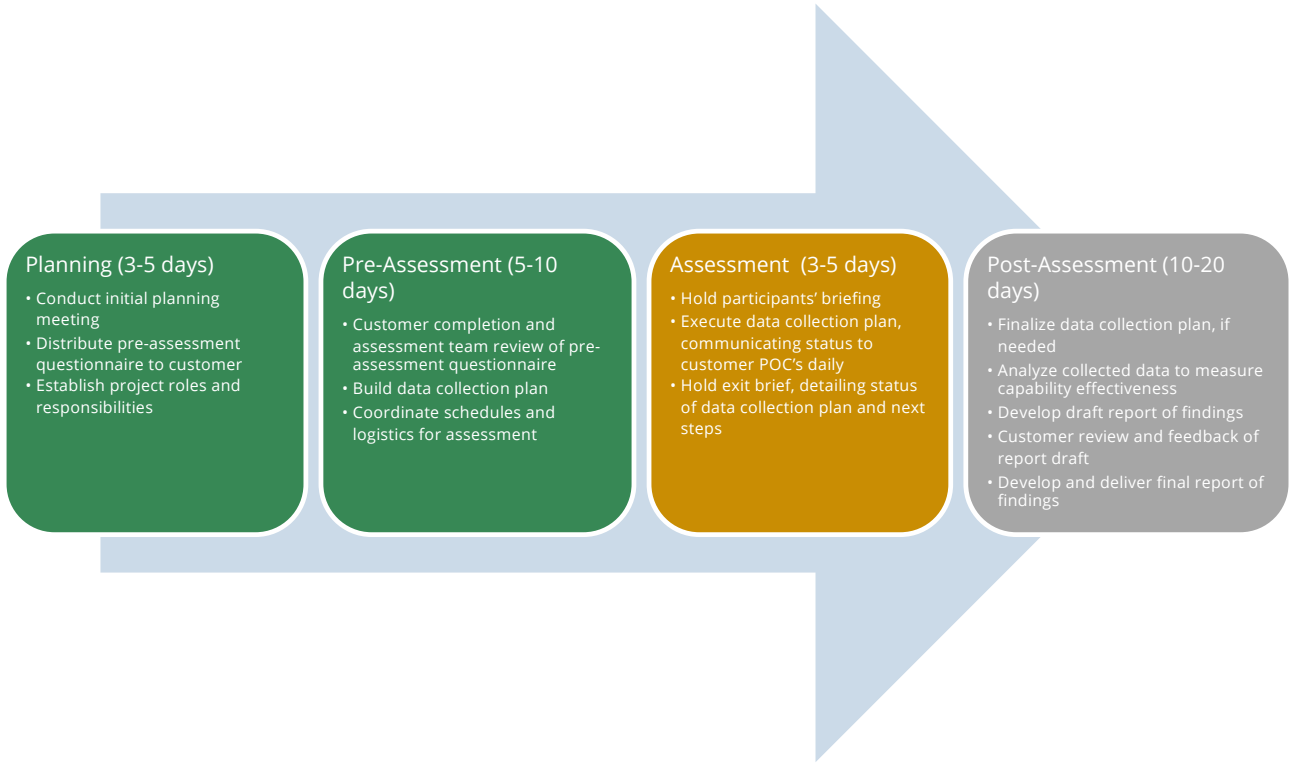
- encompass policies, practices, and technologies
- focus on all three aspects of insider threat: prevention, detection, and response

Provide a final report that enumerates

- strengths
- gaps
- prioritized recommendations

ITVA Process Flow and Timeline

Carnegie Mellon University Software Engineering Institute



Data Collection

Carnegie Mellon University Software Engineering Institute

XX documents provided and reviewed pre-assessment
XX additional documents requested and received during on-site
XX documents total

XX total on-site interviews conducted <Dates>

Collect and analyze **evidence** that supports the absence or presence of indicators

- Review of documents that describe existing processes and procedures
- Interviews with personnel that perform key activities
- Direct observations of capability (e.g. tool demonstrations)

Minimum standards for evidence provide confidence in the capability level scoring

- 1 document + 1 observation
- 1 document + 2 interviews
- 1 observation + 2 interviews
- 3 interviews

Q&A / Open Discussion

Carnegie Mellon University Software Engineering Institute