

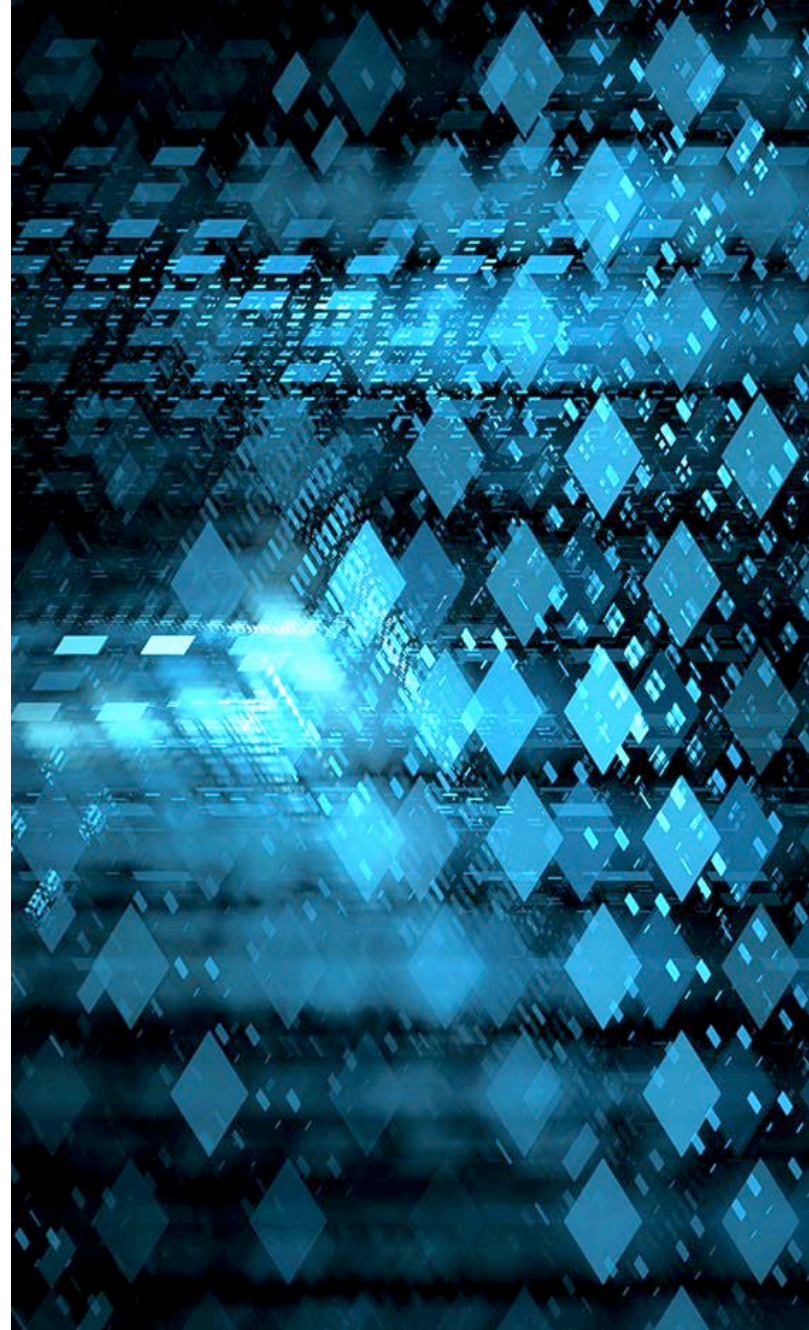
Insider Threat Program Evaluation (ITPE)

Insider Threat Vulnerability Assessment (ITVA)

Overview

CERT Insider Threat Center –
www.cert.org/Insider_Threat

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Notices

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon®, CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Introduction to the CERT Insider Threat Center

What Is the CERT Insider Threat Center?

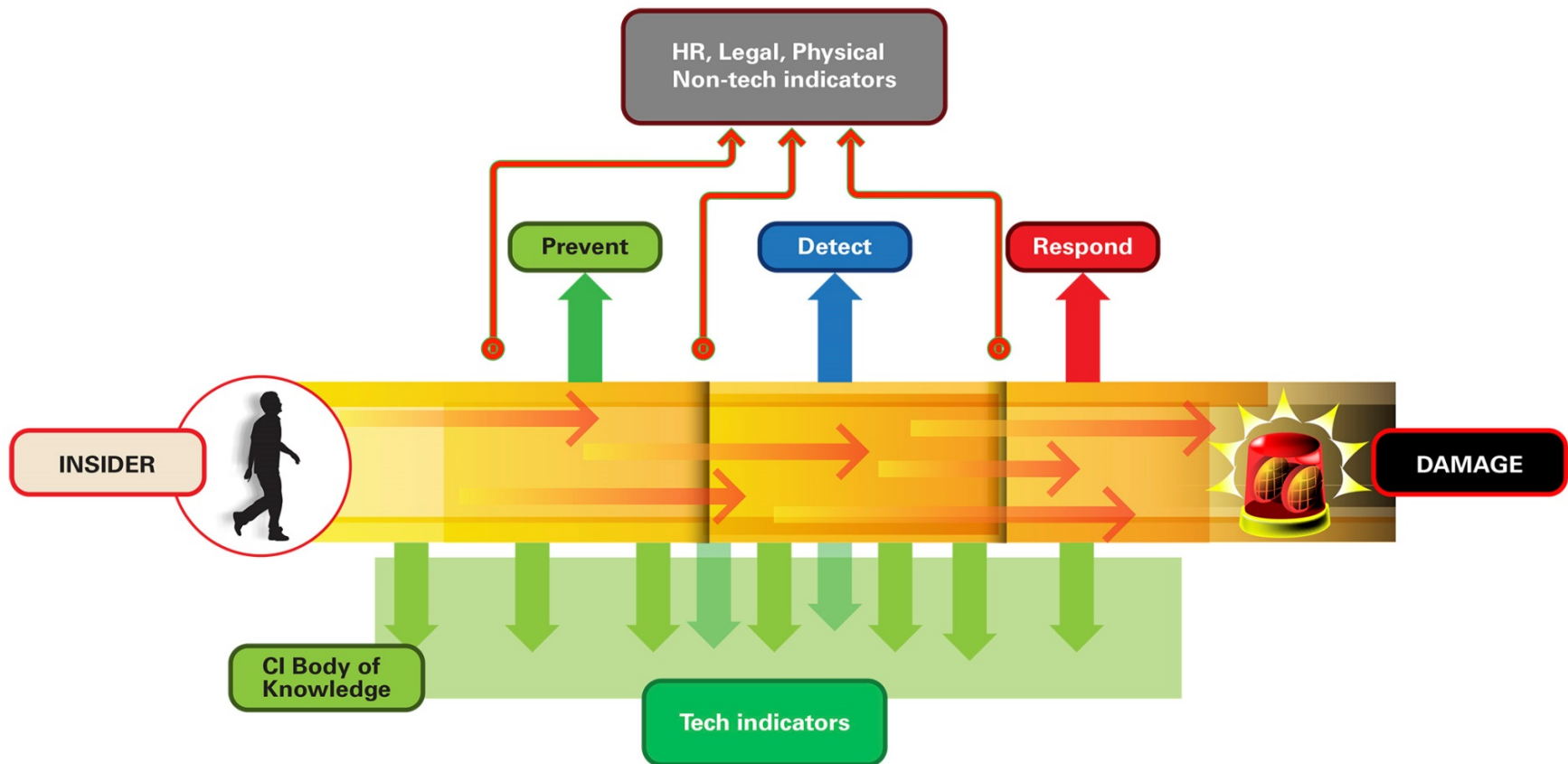
Center of insider threat expertise

Began working in this area in 2001
with the U.S. Secret Service

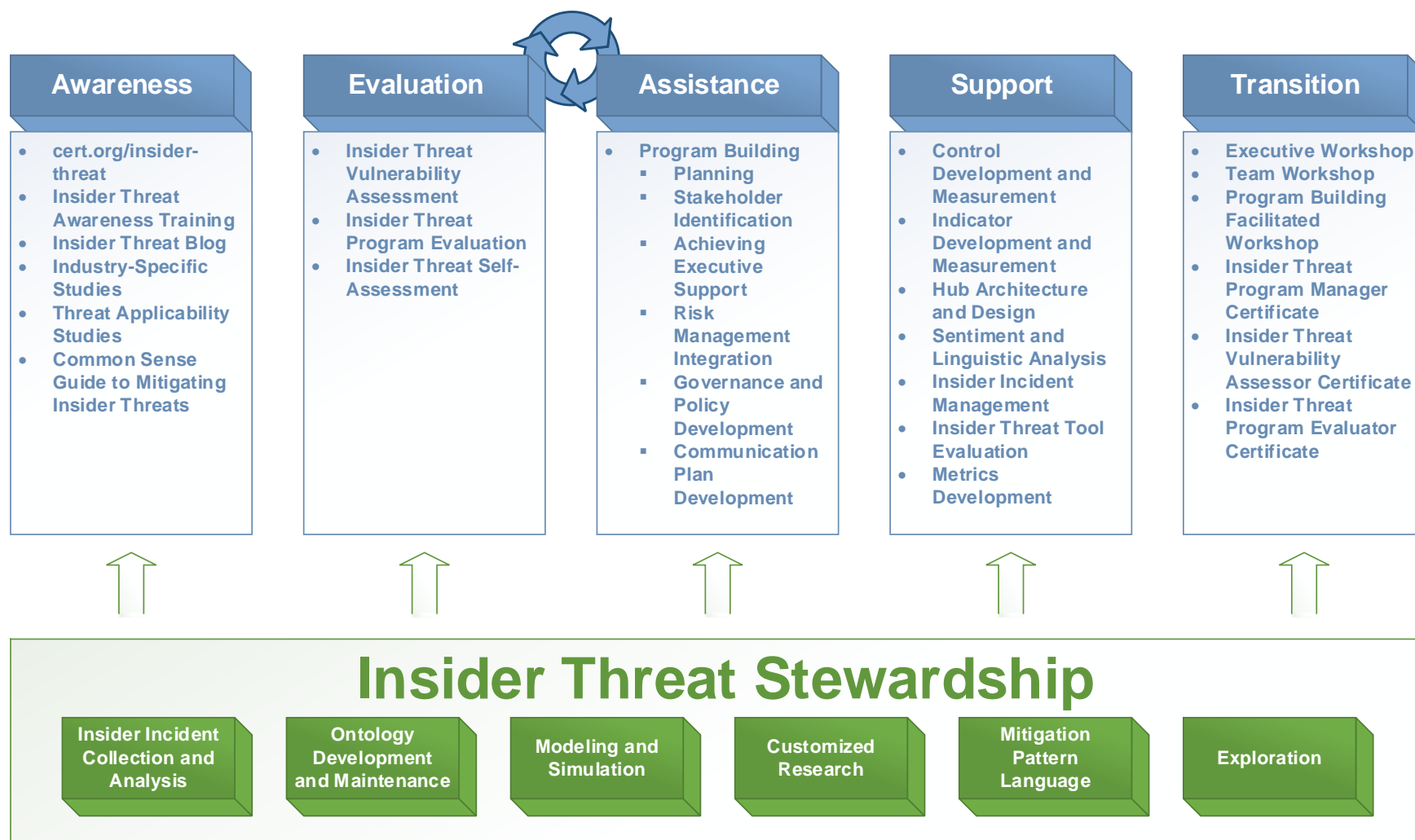


Our mission: The CERT Insider Threat Center conducts empirical research and analysis to develop and transition socio-technical solutions to combat insider cyber threats.

CERT Insider Threat Center Objective



Our Insider Threat Portfolio



CERT Insider Threat Center Assessment Types

CERT Insider Threat Center Assessment Instruments

The CERT Insider Threat Center developed two types of Insider Threat related assessment instruments:

- The Insider Threat Program Evaluation (ITPE)
- The Insider Threat Vulnerability Assessment (ITVA)

We are in the planning stages of a certificate program for licensing and learning how to conduct the ITPE.

We currently have the certificate program for the ITVA.

The Evaluations Have a Different Focus and Purpose -2

The ITPE

- Benchmarks an insider threat program against our criteria built on the National Insider Threat Task Force (NITTF) minimum standards and CERT Insider Threat Center, government, and industry best practices
- Looks at the organization's program via an enterprise perspective

The Assessments Have a Different Focus and Purpose -1

The ITVA

- Is more narrowly focused on a particular part of the organization
- Specifically looks at critical assets and business processes that support key services related to the mission of the organization
- Looks across a broad range of potential vulnerabilities that might impact the system, asset, or process being assessed
- Is limited to only areas of concern observed in the hundreds of cases in the CERT insider threat database

An organization may have good controls and processes in place for certain assets and services but not others. This is why the ITVA is a focused assessment, not an enterprise-wide one.

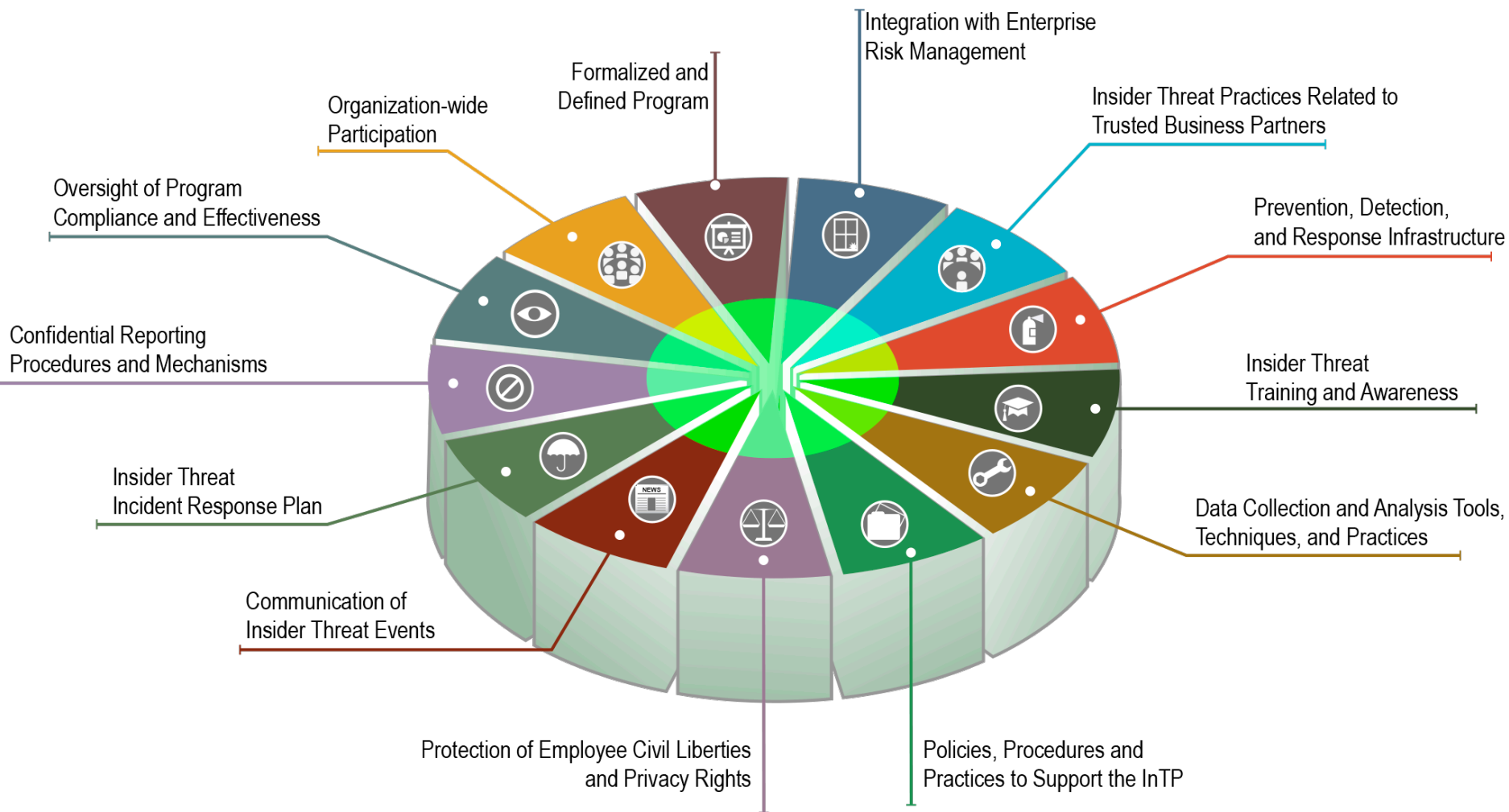
Overview of ITPE

ITPE Purpose and Benefit

The Insider Threat Program Evaluation assesses the robustness of the organization's program to prevent, detect, and respond to insider threats and provides recommendations for enhancing the program's effectiveness.

The long-term benefit is to assist organizations in reducing exposure to damage from potential insider threats.

Evaluation of Program Components*



ITPE Workbooks

Program Management

Personnel and Training

Collection and Analysis

Human Resources and Legal

ITPE Capabilities

Program Management	Personnel and Training	Collection and Analysis	Personnel and Training Human Resources and Legal
Formalized Program	Organization-wide Training	Access Control	Employee Lifecycle: Hiring, Onboarding, and Separation
InTP Policy	InTP Team Composition	Modification of Data or Disruption of Services or Systems	Employee Investigations
Insider Threat Response Plan	Insider Threat Awareness Training for Organization	Unauthorized Access, Download, or Transfer of Assets	Confidential Reporting
Insider Threat Program Communication Plan	InTP Team Training	Detection and Identification	Identifying At-Risk Employees
ERM Integration	Role-based Training for Organization	Incident Response	Intellectual Property
Critical Asset Identification	Manager and Supervisor Training	Termination	Employee Support Programs
InTP Governance			InTP Access to HR Information
Quality, Effectiveness, and Performance of the InTP			User Monitoring Policy
			Physical and Personnel Security

ITPE Indicators Often Have Special Notations

Indicators within capabilities that are marked with a

- “[NITTF]” mean that the indicator came from the NITTF minimum standards
- “[NISPOM]” are those required to meet National Industry Security Program (NISPOM) standards

Those preceded by “[For U.S. Federal Government Only]” mean

- that the indicator only applies if the organization being evaluated is a U.S. Federal government agency or department
- if not then those indicators should not be evaluated or included in the scoring.

Example of Special Indicator Notation

- ☐ InTP activities are conducted in accordance with applicable laws, whistleblower protections, civil liberties and privacy policies. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

- ☐ The InTP has a yearly budget.

Doc Rev

Dir Obs

Intvw

- ☐ [For U.S. Federal Government Only] The InTP designated senior official has submitted to the agency head an implementation plan for establishing an InTP. [NITTF] [NISPOM]

Doc Rev

Dir Obs

Intvw

Capability Examples

PM1.1: Formalized Program

- A formal insider threat program has been established.

CA2.5: User Activity Monitoring

- The organization established and maintains a program to monitor, log, and audit the activities of employees and other users on its networks and systems, based on its defined requirements and in keeping with any legal or privacy rules.

Capability Sequence # PM1.1



Capability

A formal insider threat program has been established



Activity

Establishing and institutionalizing the Insider Threat Program



Target

Organizational structure and authority



Reason

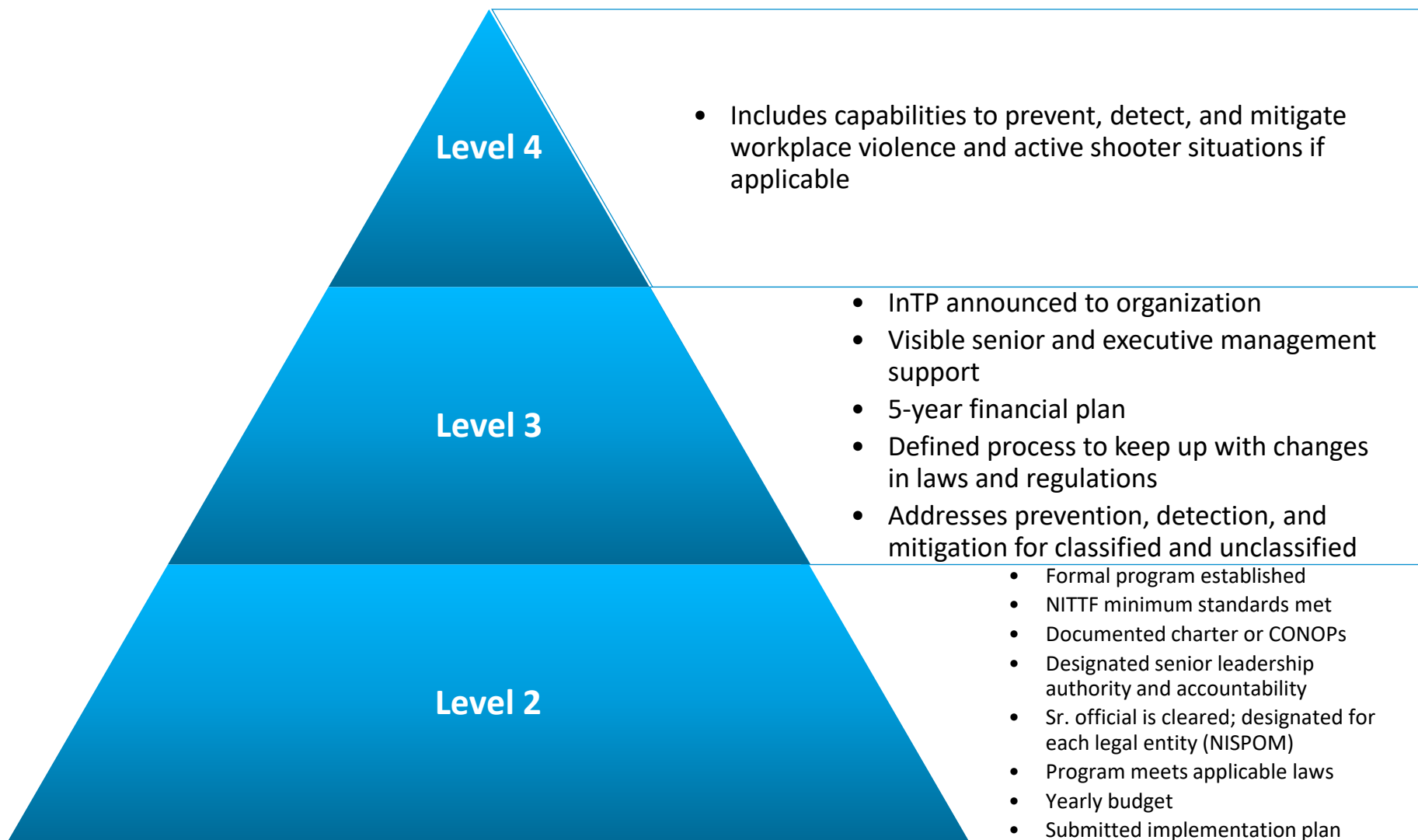
By implementing a formal InTP, the organization can be prepared to handle an insider threat in an effective, confidential, and timely manner. .



Specific Activities

Visible management support; designated senior official; built in consultation with legal, civil liberties, and privacy officials; defined authority; assigned staff; yearly budget; defined charter

Capability Sequence # PM1.1



Capability Sequence # CA2.5



Capability

The organization monitors user activity on its networks and systems.



Activity

The organization established and maintains a program to monitor, log, and audit the activities of employees and other users on its networks and systems, based on its defined requirements.



Target

Monitoring performed on classified and unclassified systems as appropriate.



Reason

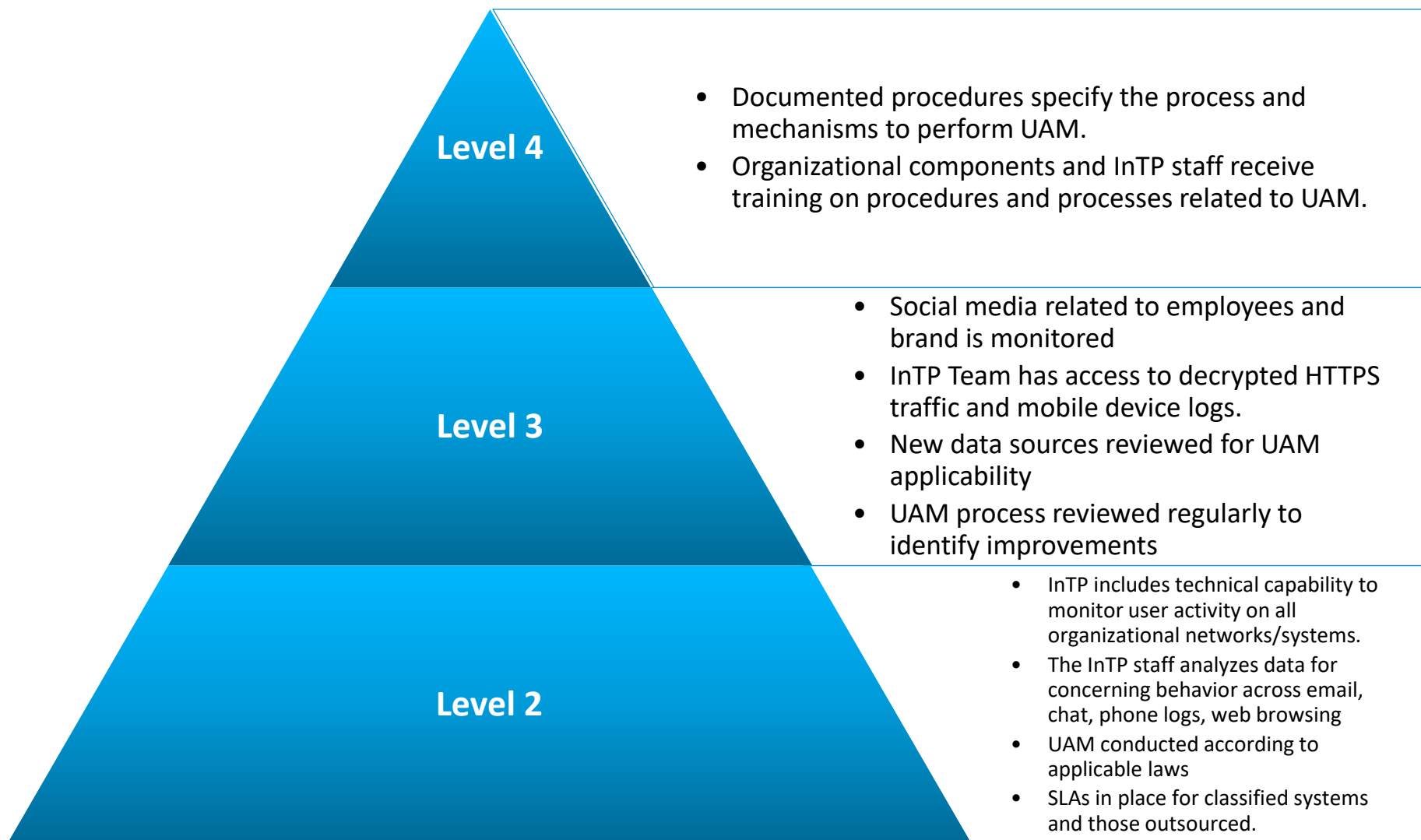
Insiders may insert malicious code during software development.



Specific Activities

Ability to identify anomalous or suspicious insider behavior; detect investigate, and mitigate quickly.

Capability Sequence # CA2.5



Overview of ITVA

ITVA Purpose

the Insider Threat Vulnerability Assessment (ITVA) method evaluates an organization's preparedness to prevent, detect, and respond to insider threats.

The ITVA is focused on identifying insider threat vulnerabilities in a very broad context, across both classified and unclassified systems, data, and processes.

It looks for vulnerabilities related to IT Sabotage, IP Theft, and Fraud.

The methodology is designed to review policies, practices, controls, and technologies in place that are focused on particular critical business services and their supporting processes.

ITVA Benefit

To help identify potential vulnerabilities that can be exploited by malicious insiders

To provide the organization with business justification for implementing improvements and revising resources based on the output

The ITVA long-term benefit is to assist organizations in reducing exposure to damage from potential insider threats.

General Scope of ITVA

Vulnerability assessment only

- Not an audit.
- Not a compliance exercise or performance review.
- Not a maturity model
- Not looking for malicious insiders.
- Only assessing how well an organization would do against the vulnerabilities exploited in the CERT database cases.

Intentional - Only

- The ITVA is focused on “intentional” insider activities.
- It does not include vulnerabilities exploited unintentionally (accidentally) by end-users at this time.

Vulnerabilities are both **Technical** and **Behavioral** including but not limited to

- Psychological
- Process-based
- Policy-based
- Control-based

ITVA Workbooks

Data Owners

Human Resources

Legal/Contracts

Physical Security

Information Technology

Software Engineering

Trusted Business Partners

ITVA Capabilities

Workbooks

Data Owners	Human Resources	Information Technology	Legal	Physical Security	Software Engineering	Trusted Business Partners
Access Control	Recruitment	Access Control	Agreements to Protect Sensitive Information	Facility Security	Technical Policies and Agreements	Screening/Hiring of Applicants
Modification of Data, Systems, or Logs	Policies and Practices	Modification of Data or Disruption of Services or Systems	Restrictions on Outside Employment	Physical Asset Security	Modification of Data or Systems	Management of Business Partners
Unauthorized Access, Download, or Transfer of Assets	Training and Education, Evaluation	Unauthorized Access, Download, or Transfer of Assets	Employee Behaviors in the Workplace		Asset Management	Asset Management
Incident Response	Policy and Practice Monitoring and Enforcement Programs	Detection and Identification	Conditions of Hire			Incident Response
Termination	Enforcement and Termination	Incident Response	Property Lending Agreements			Contractor/ Business Partner Agreements
		Termination	Contractor/ Business Partner Agreements			

Capability Examples

SE1.4: Software Development Peer Review

- The organization uses peer reviews to prevent, detect, and respond to malicious code insertion during software development.

LG1.6: Intellectual Property Ownership

- The organization has policy regarding ownership of the organization's intellectual property (IP) to reduce the likelihood of disputes and insider threats.

Capability Sequence # SE1.4



Capability

The organization uses peer reviews to prevent, detect, and respond to malicious code insertion during software development.



Activity

Conducting peer reviews



Target

Software code



Reason

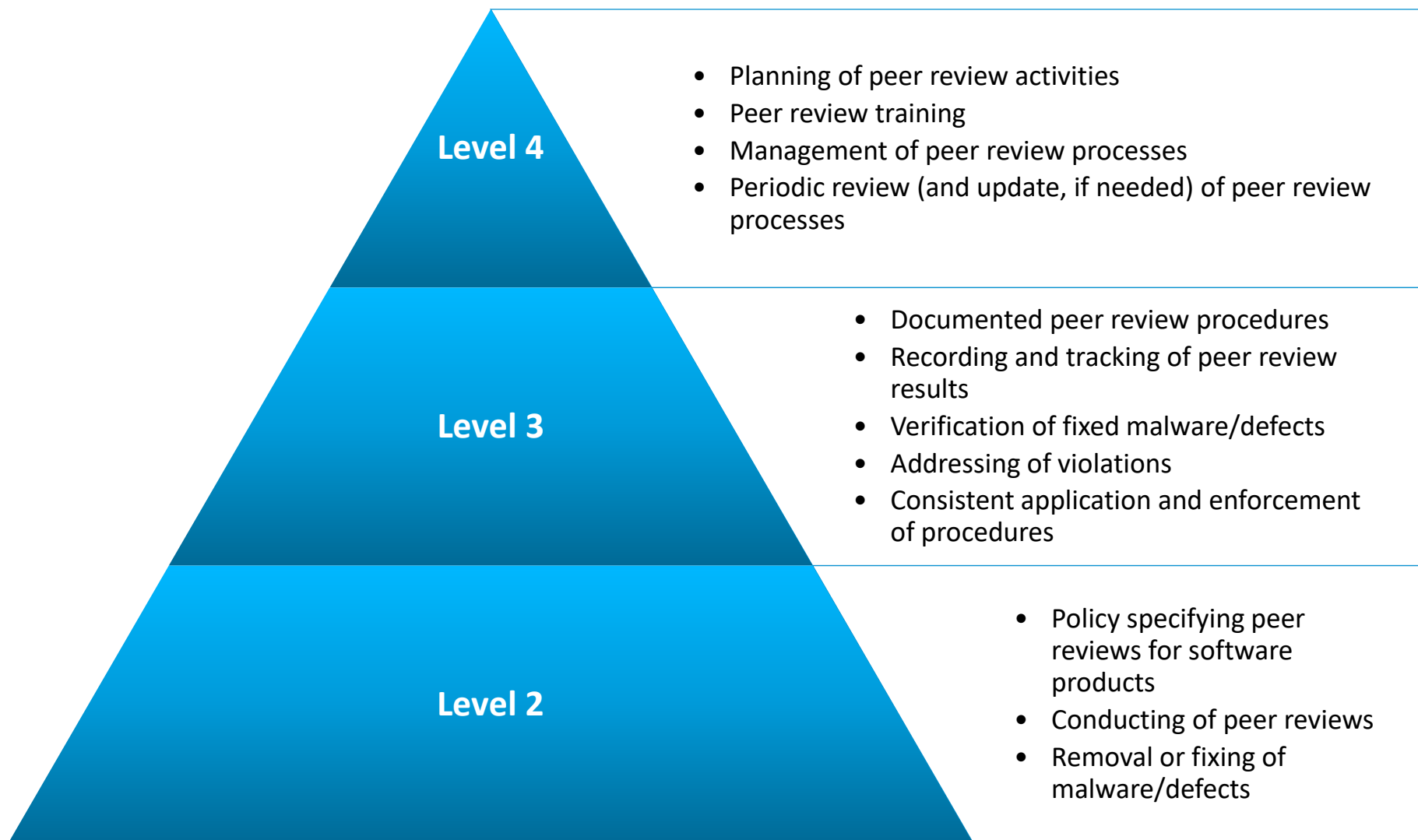
Insiders may insert malicious code during software development.



Specific Activities

Includes policies, procedures, and training of developers on conducting peer reviews for malware detection

Capability Sequence # SE1.4



Capability Sequence # LG1.6



Capability

The organization has policy regarding ownership of the organization's intellectual property (IP) to reduce the likelihood of disputes and insider threats.



Activity

Detecting and preventing IP theft



Target

Intellectual property agreements




Reason

Communication and enforcement of IP agreements aid in prevention and response to the theft of IP.



Specific Activities

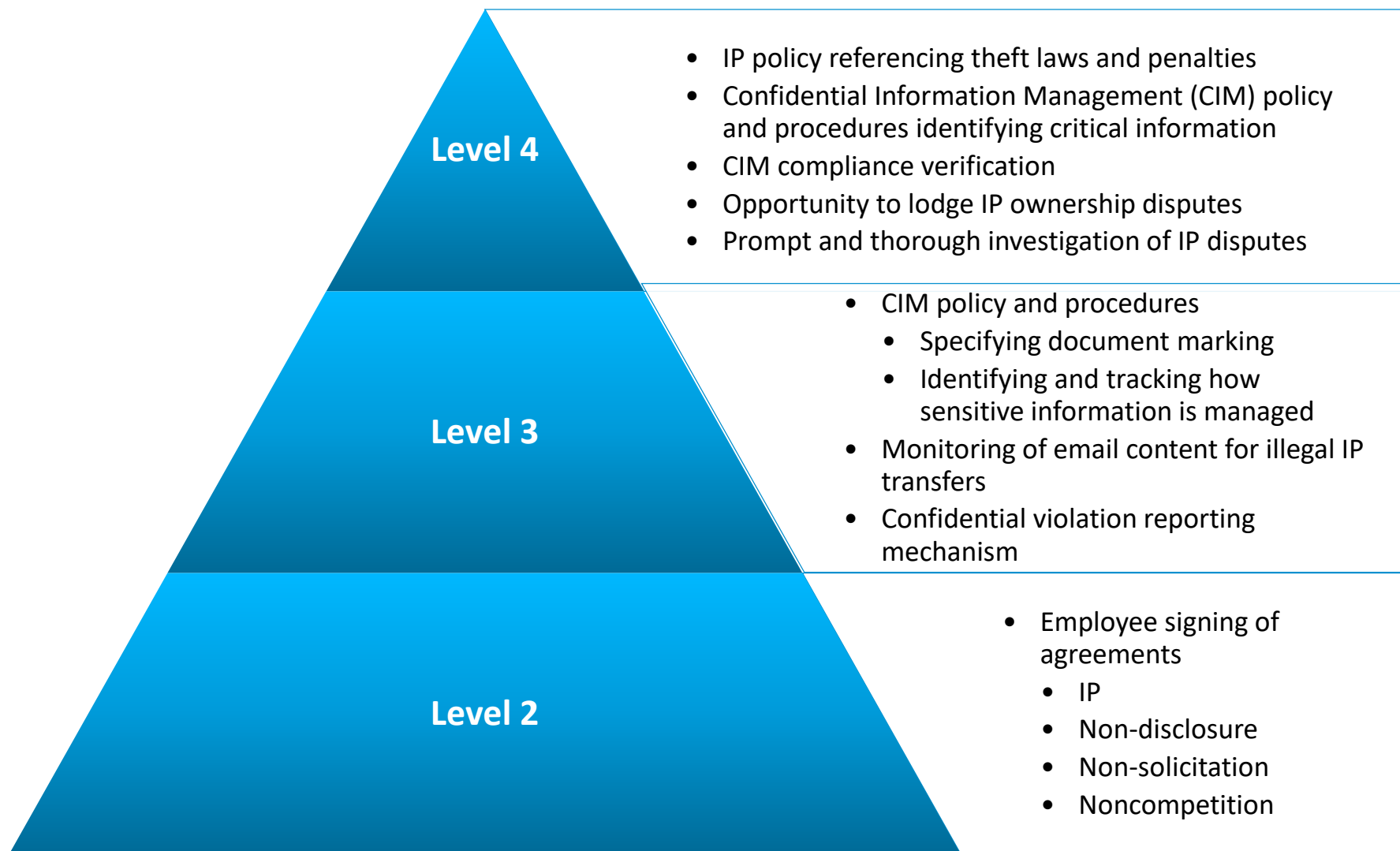
Includes non-disclosures, non-competes, appropriate marking of IP, and reporting of violations



Warnings/Notes

Caution: Policies alone are insufficient without communication/agreement to the policies.

Capability Sequence # LG1.6



General Methodology

Methodology is Similar

The basic methodology is followed for both assessment types.



The Process has four activities:

1. Planning
2. Pre-work (Initial documentation review, data gathering questions, data collection planning)
3. On-site Data Collection (3-5 days)
4. Post-work
 - Develop summary report (**~10 days**)
 - Review and finalization (**10-20+ days**)

Workbook Format and Scoring Rules

Workbook Terminology -1

Capability

- A capability is a question that determines whether an organization has the appropriate controls or practices in place to address a specific vulnerability.

Level

- Levels are measures of preparedness for preventing, detecting, and responding to insider threats or specific vulnerabilities that may be exploited by insiders.
- Most capabilities have four levels.
- Each level within a capability has a set of indicators that must be met to achieve that level.

Workbook Terminology -2

Indicators

- Individual questions related to controls, practices, processes, or other activities that must be met and substantiated to meet a level.

Score

- Capability scores are given in terms of the level of preparedness achieved.
- The score for a capability is based on the highest level where all the indicators in that level are met.

Capability Indicator Example

Scoring Criteria

Level 1

A score of Level 1 indicates failure to meet the requirements for the higher levels.

Doc Rev

Dir Obs

Intvw

Level 2

☐ The organization has a documented policy that describes the TBP's obligation to report policy violations.

Doc Rev

Dir Obs

Intvw

Level 3

☐ The policy outlines specific reporting options and procedures.

Doc Rev

Dir Obs

Intvw

Level 4

☐ The organization or contracting agency trains TBPs on the reporting procedures and requirements.

Doc Rev

Dir Obs

Intvw

☐ The organization follows-up on policy violation reports from TBPs.

Doc Rev

Dir Obs

Intvw

Capability Scores

Capability scores are the Level that the organization is determined to be at:

- Level 1
- Level 2
- Level 3
- Level 4

Scores for capabilities can also be

- Not Applicable (NA) – The capability is out of scope, or is not something that would be provided by the organization assessed.
- Not Observed (NO) – The capability may be provided, but the assessment team was not able to talk to anyone or collect evidence to evaluate the capability.

Scoring Levels Are Different for Each Assessment

ITPE Scoring Levels

- Level 4 – Exceptional measures or practices are in place.
- Level 3 – Above average measures and practices are in place.
- Level 2 – The organization meets the NITTF minimum standards and general CERT Insider Threat Center best practices
- Level 1 – Inadequate or no practices are in place.

ITVA Scoring Levels

- Level 4 – Exceptional countermeasures are in place to address vulnerabilities. The organization prevents, detects, and responds to threats.
- Level 3 – Adequate countermeasures are in place. The organization detects and responds to threats.
- Level 2 – Minimal countermeasures are in place. The organization detects threats.
- Level 1 – Inadequate or no countermeasures are in place.

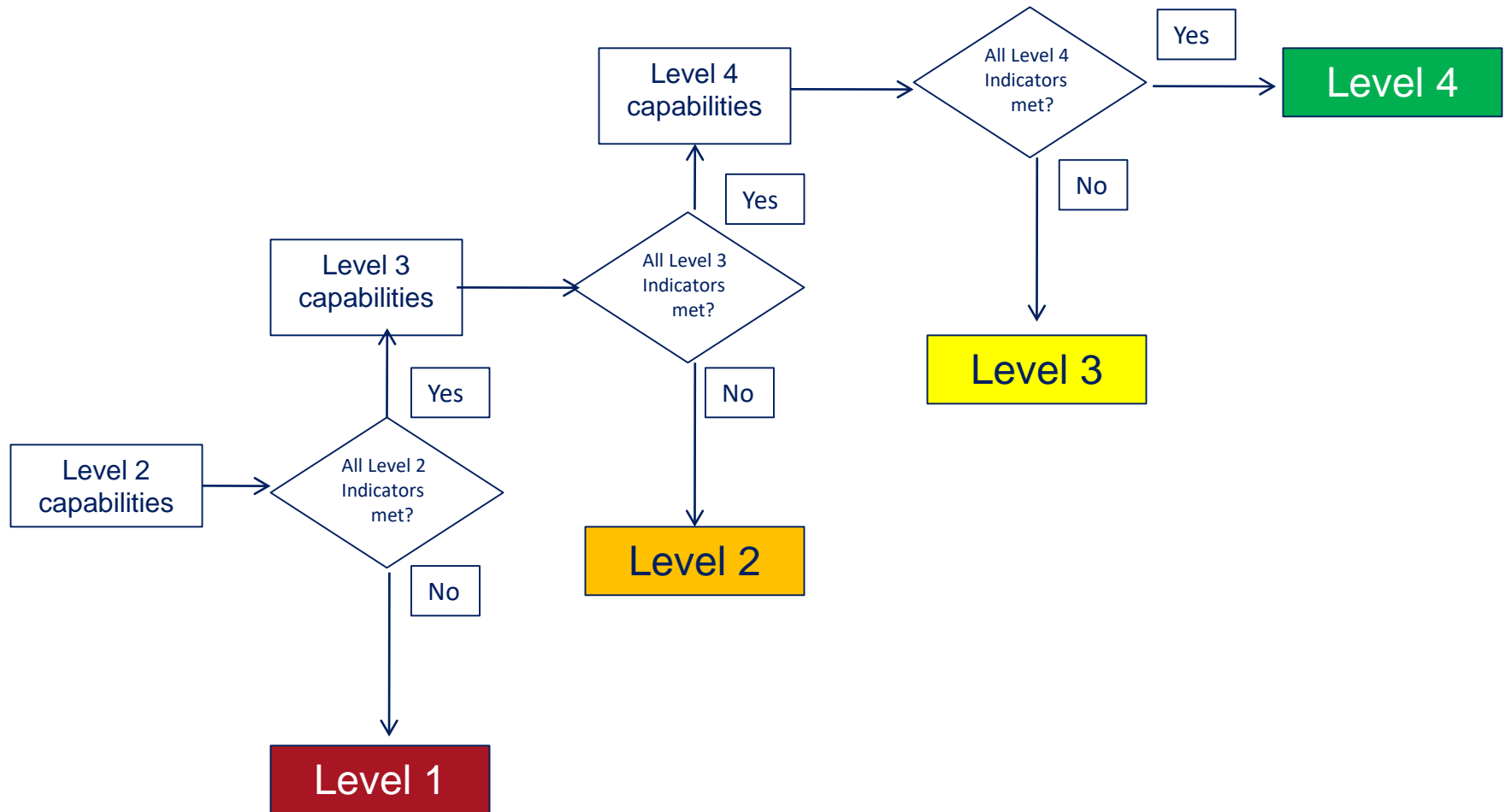
Capability Scoring

After all the indicators for a capability have been evaluated and substantiated, then the capability can be scored.

A capability is scored based on the indicators that are met.

To achieve a specific level of preparedness, **ALL** the indicators in that level must be met **AND** all the indicators in the preceding levels **MUST ALSO** be fully met.

Capability Scoring Flowchart



Substantiation of Evidence

Capability values are assigned based on the evidence collected. Evidence must be substantiated according to the following rules that require either

1 document + 1 observation

1 document + 2 or more interviews

1 observation + 2 or more interviews

3 or more interviews (if interviews alone)

If there are problem area additional substantiation is obtained.

Sample ITVA Scoring Matrix

Capability ID	Description	Score	Rationale
DO1.02	The organization ensures that critical processes are not completed by a sole individual without the appropriate level of checks and balances.		
DO4.02	The organization manages employees' access after they announce their pending resignation or termination.		
HR1.01	The organization confirms the identities and personal and professional histories of job candidates.		
HR1.18	The organization has documented policy for targeted monitoring.		

Sample Report Content

Assessment reports can include

- determination of which capabilities are
 - done well
 - not done at all
 - need some improvement
- identification of key observations obtained during assessment activities
 - key strengths
 - key gaps
 - constraints
- additional components or follow-on components based on assessment team resources and mission could include
 - improvements and recommendations
 - prioritized implementation plan
 - roadmap

Sample ITVA Report Outline

Executive Summary

Introduction

- ITVA Background
- Scope
- Method
- Structure of this Report

Data Owners

- Observations
- Recommendations

Human Resources

- Observations
- Recommendations

Information Technology

- Observations
- Recommendations

Legal

- Observations
- Recommendations

Physical Security

- Observations
- Recommendations

Software Engineering

- Observations
- Recommendations

Trusted Business Partners

- Observations
- Recommendations

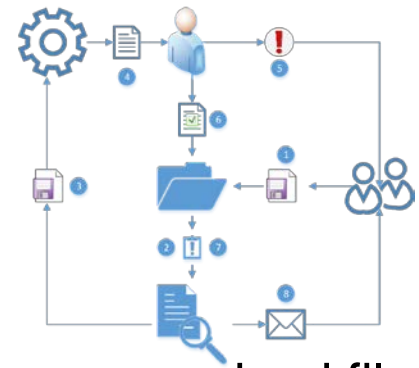
Appendices

- Appendix A: Scores for Data Owners
- Appendix B: Scores for Human Resources
- Appendix C: Scores for Information Technology
- Appendix D: Scores for Legal
- Appendix E: Scores for Physical Security
- Appendix F: Scores for Software Engineering
- Appendix G: Scores for Trusted Business Partners

For Licensed Partners

There is a very specific report development process used for licensed partners:

- The licensed partner database manager exports an anonymized file from the JAT containing the indicator and capability scores for the capabilities assessed.
 - There is a special export option for this.
 - A .csv file is created for exporting
- This file is uploaded ITVA part of the Partner Network Portal (PNP) .
- The CERT Insider Threat Center obtains the exported file and generates the draft assessment report.
- A quality review is completed by the CERT Insider Threat Center.
- Any problems or issues found are discussed with licensees.
- A copy of the draft report is put into your folder on the PNP for downloading.
- Additional information can also be added by you to the standardized body of the report that you downloaded.



Questions and Discussion

