# Assessing Information Security Continuous Monitoring (ISCM) Programs

Federal Computer Security Managers' Forum
February 6, 2020

**Chad Baer**

Cybersecurity and Infrastructure Security Agency

**Vicky Yan Pillitteri**

National Institute of Standards and Technology

# Agenda

- Background and Key Questions
- Overview of Information Security Continuous Monitoring (ISCM)
- ISCM Program Assessments using draft NIST SP 800-137A
- Public comment process and next steps
- Q&A

# Background

- **CISA** developed **ISCM Assessment (ISCMA)** with support from the Continuous Diagnostics and Mitigation (CDM) Program
  - Objective: help agencies articulate “how they should be continuously monitoring their organizations”
- Assessment intended to serve as a view into an organizations’ **readiness to accept, manage, and sustain an effective continuous monitoring program**, to include their DHS CDM platform
- Pilots of the ISCMA proved the efficacy of the evaluation to identify potential areas for improvement within the organizational approach to ISCM

# Key Questions

ISCM Assessment aimed to answer:

- Has **agency senior leadership** adequately described the **organization's objectives for continuous monitoring**; the programs' **strategic purpose** and the **people, processes, tools and governance** they will commit to achieve those goals?
- Has agency management adequately **designed a program** that will **achieve the ISCM strategic goals** across the entire breadth and depth of the agency and its subordinate organizations, and can the program endure across changes?
- Are **all parts** of the agency **executing the program** as designed?
- **If an effective and efficient ISCM program has been defined, established, and implemented to be sustainable and endure organizational changes.**

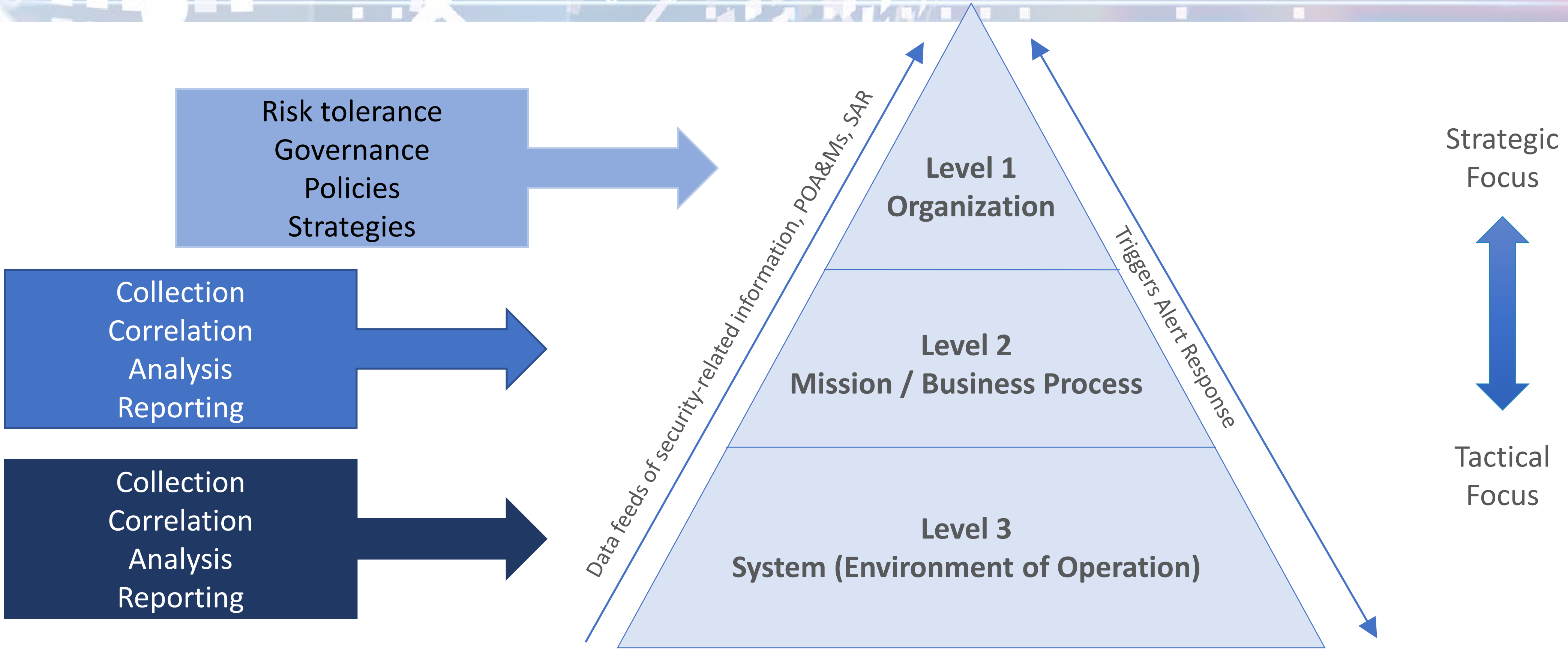
# Overview of ISCM

**Information security continuous monitoring (ISCM)** is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

# Overview of ISCM: ISCM Strategy

- Is grounded in a clear understanding of **organizational risk tolerance**
- Helps **set priorities and manage risk consistently** throughout the organization
- Includes metrics that provide **meaningful indications of security status** at all organizational levels
- Ensures **continued effectiveness** of **all controls**
- Verifies **compliance with information security requirements**
- Is informed by all organizational IT assets and helps to maintain **visibility into the security of the assets**
- Ensures **knowledge and control of changes** to organizational systems and environments of operation
- Maintains awareness of **threats and vulnerabilities**

# Overview of ISCM: Organization-Wide ISCM



Risk tolerance
Governance
Policies
Strategies

Collection
Correlation
Analysis
Reporting

Collection
Correlation
Analysis
Reporting

Data feeds of security-related information, POA&Ms, SAR

Level 1
Organization

Level 2
Mission / Business Process

Level 3
System (Environment of Operation)

Triggers Alert Response

Strategic Focus

Tactical Focus

**Three Levels of Organization-Wide Risk Management**

# Overview of ISCM: ISCM Process

**Define** an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.

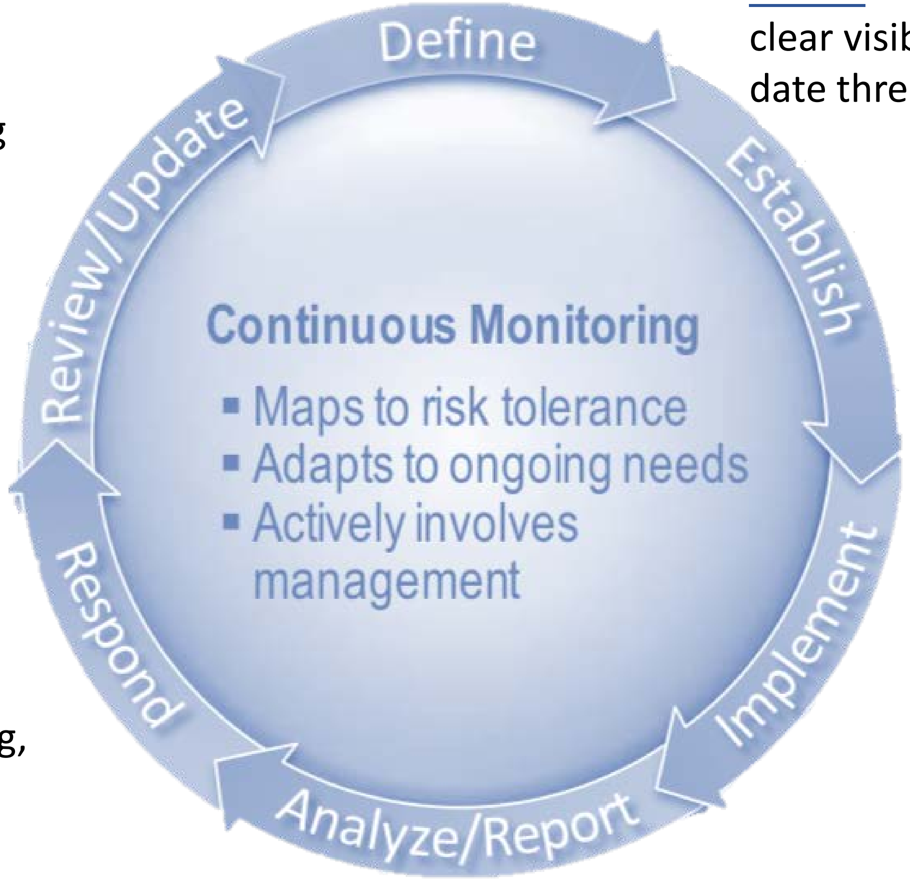
**Establish** an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.

**Implement** an ISCM program and collect the security-related information required for metrics, assessments, and reporting.

**Analyze** the data collected and **Report** findings, determining the appropriate response.

**Respond** to findings with mitigating activities or acceptance, transference/sharing, or avoidance/rejection.

**Review and Update** the monitoring program, adjusting the ISCM strategy and maturing measurement capabilities.



CISA
CYBER+INFRASTRUCTURE

NIST National Institute of Standards and Technology U.S. Department of Commerce

# ISCM Program Assessments

**Draft NIST SP 800-137A, *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment***
**https://csrc.nist.gov/publications/detail/sp/800-137a/draft**

**Goal:** Provide an organization with a **repeatable and consistent methodology to assess ISCM programs** that results in actionable recommendations to improve the ISCM program.

ISCM program assessment results include:

- an indication of how **well the assessed organization** (entire organization, mission/business process, or system) **meets the evaluation criteria**
- indications of **ISCM program adequacy and consistency**
- **recommendations for** ISCM program design, implementation, operation, and governance that may need **improvement**.

⚠

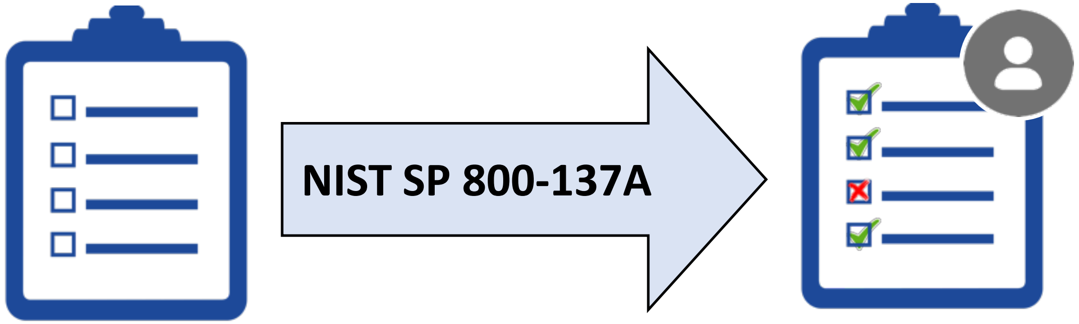
NIST SP 800-137A Assessment Elements are included in a **separate .xlsx catalog** available under "supplemental materials"

CISA
CYBER+INFRASTRUCTURE

NIST National Institute of Standards and Technology U.S. Department of Commerce

# Properties of ISCM Program Assessment

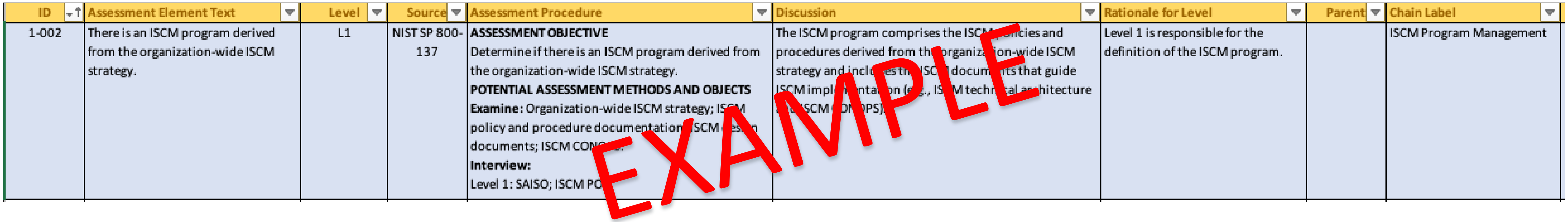
1. Focus 1 ISCM Process Step at a time
2. Each assessment element applicable to only one ISCM Process Step
3. Use readily available security-related information
4. Avoid re-test/re-assessment of controls (out of scope)
5. Assess automated and manual ISCM methods
6. Trace each assessment element to source
7. Can add/modify/exclude assessment procedures as necessary
8. Apply to any organization
9. Technology/implementation neutral
10. Results lead to actionable recommendations
11. Strategic and programmatic perspective
12. Guidance for repeatable assessments



CISA
CYBER+INFRASTRUCTURE

NIST National Institute of Standards and Technology
U.S. Department of Commerce

# ISCM Program Assessment Criteria



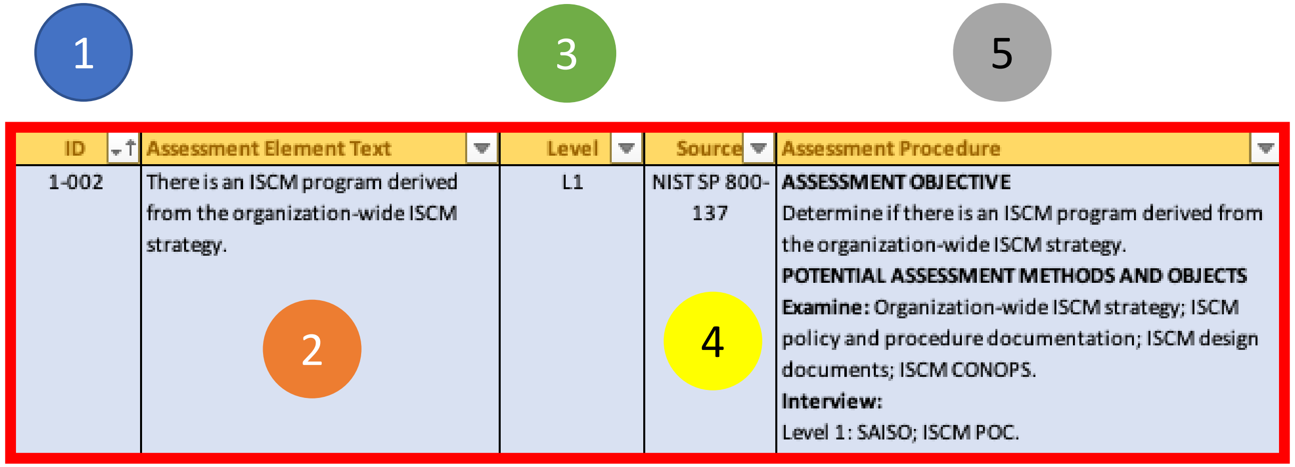
| ID | Assessment Element Text | Level | Source | Assessment Procedure | Discussion | Rationale for Level | Parent | Chain Label |
|---|---|---|---|---|---|---|---|---|
| 1-002 | There is an ISCM program derived from the organization-wide ISCM strategy. | L1 | NIST SP 800-137 | **ASSESSMENT OBJECTIVE**<br>Determine if there is an ISCM program derived from the organization-wide ISCM strategy.<br>**POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine:** Organization-wide ISCM strategy; ISCM policy and procedure documentation; ISCM design documents; ISCM CONOPS.<br>**Interview:**<br>Level 1: SAISO; ISCM PO | The ISCM program comprises the ISCM policies and procedures derived from the organization-wide ISCM strategy and includes the ISCM documents that guide ISCM implementation (e.g., ISCM technical architecture and ISCM CONOPS). | Level 1 is responsible for the definition of the ISCM program. | | ISCM Program Management |

EXAMPLE

CISA
CYBER+INFRASTRUCTURE

NIST National Institute of Standards and Technology
U.S. Department of Commerce

# ISCM Program Assessment Criteria



| ID | Assessment Element Text | Level | Source | Assessment Procedure |
|---|---|---|---|---|
| 1-002 | There is an ISCM program derived from the organization-wide ISCM strategy. | L1 | NIST SP 800-137 | **ASSESSMENT OBJECTIVE**<br>Determine if there is an ISCM program derived from the organization-wide ISCM strategy.<br>**POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine:** Organization-wide ISCM strategy; ISCM policy and procedure documentation; ISCM design documents; ISCM CONOPS.<br>**Interview:**<br>Level 1: SAISO; ISCM POC. |

## Assessment Element Attributes

1 Unique ID for each Assessment Element

2 Assessment Element Text

3 Applicable Risk Management Level
(L1 – Organization; L2 - Mission/Business Function; L3 – System)

4 Assessment Element Source

5 Assessment Procedure
(Assessment Objective, Potential Assessment Methods and Objects)

# ISCM Program Assessment Criteria

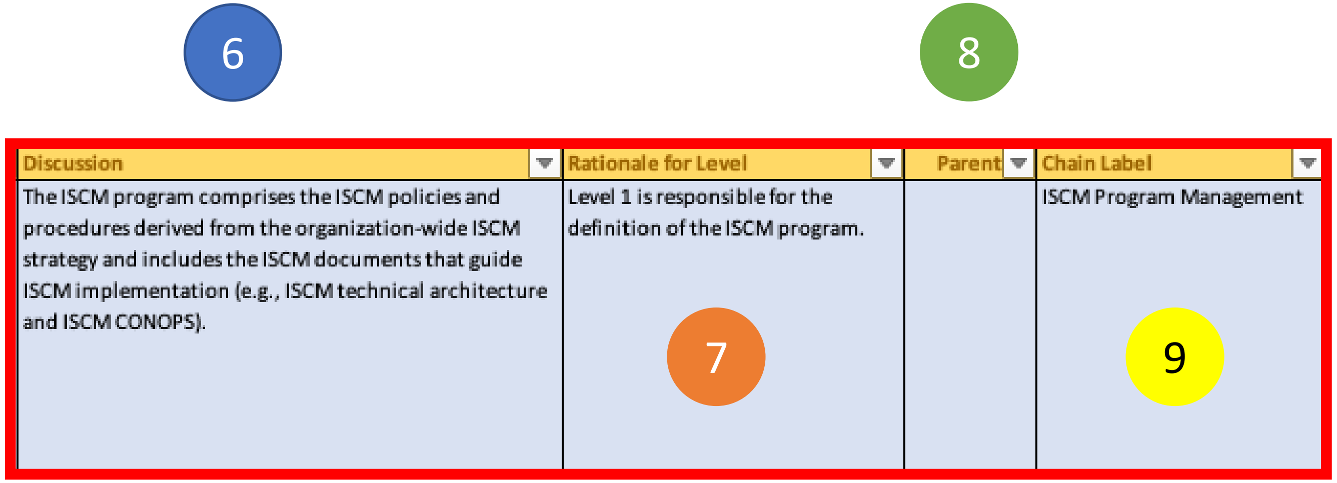
## Assessment Element Attributes

6 Discussion

7 Rationale for Level (Related to 3)

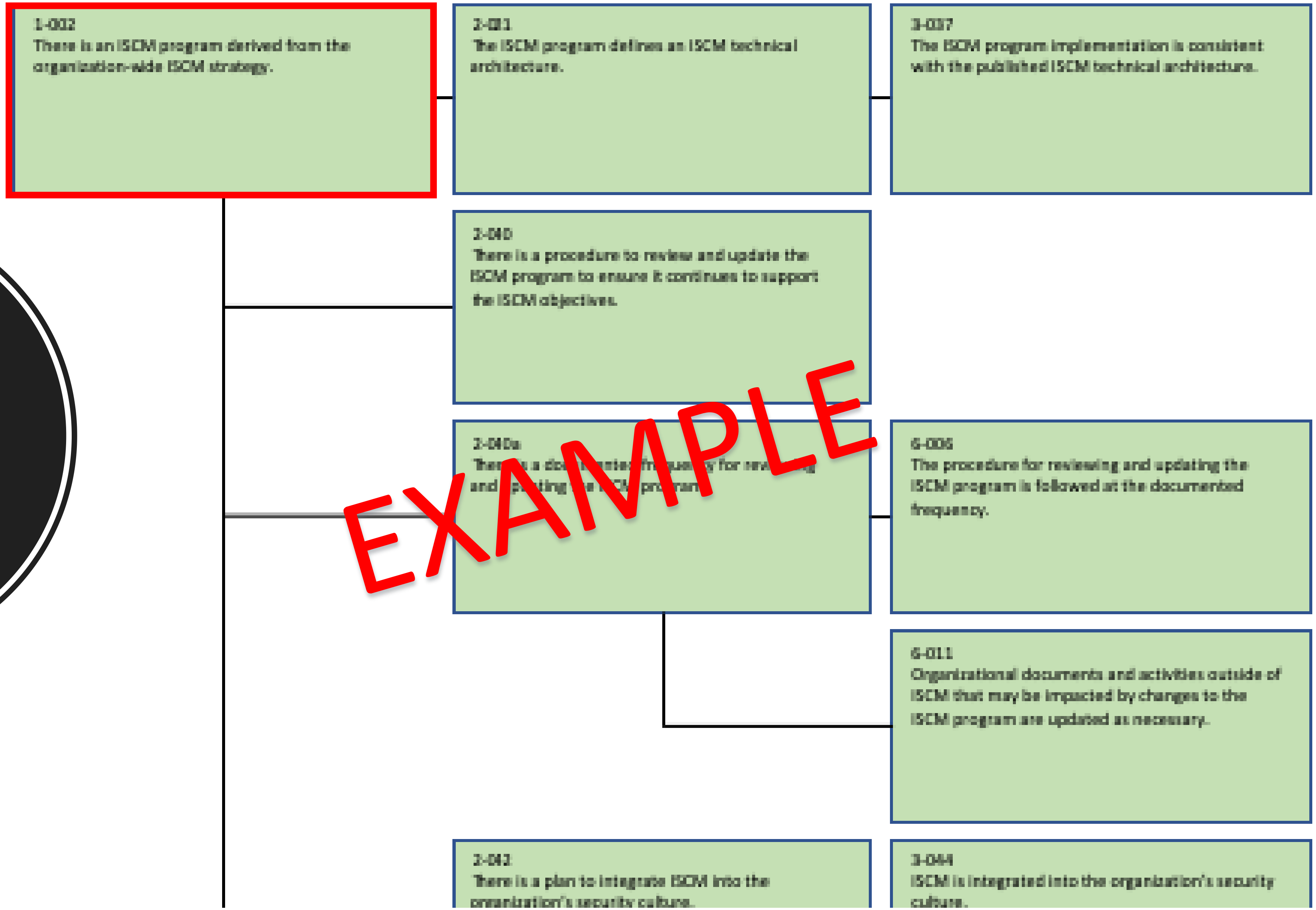
8 Parent

9 Chain Label



| Discussion | Rationale for Level | Parent | Chain Label |
|---|---|---|---|
| The ISCM program comprises the ISCM policies and procedures derived from the organization-wide ISCM strategy and includes the ISCM documents that guide ISCM implementation (e.g., ISCM technical architecture and ISCM CONOPS). | Level 1 is responsible for the definition of the ISCM program. | | ISCM Program Management |

# Traceability of Assessment Elements



1-002
There is an ISCM program derived from the organization-wide ISCM strategy.

2-031
The ISCM program defines an ISCM technical architecture.

3-037
The ISCM program implementation is consistent with the published ISCM technical architecture.

2-040
There is a procedure to review and update the ISCM program to ensure it continues to support the ISCM objectives.

2-040a
There is a documented frequency for reviewing and updating the ISCM program.

6-006
The procedure for reviewing and updating the ISCM program is followed at the documented frequency.

6-011
Organizational documents and activities outside of ISCM that may be impacted by changes to the ISCM program are updated as necessary.

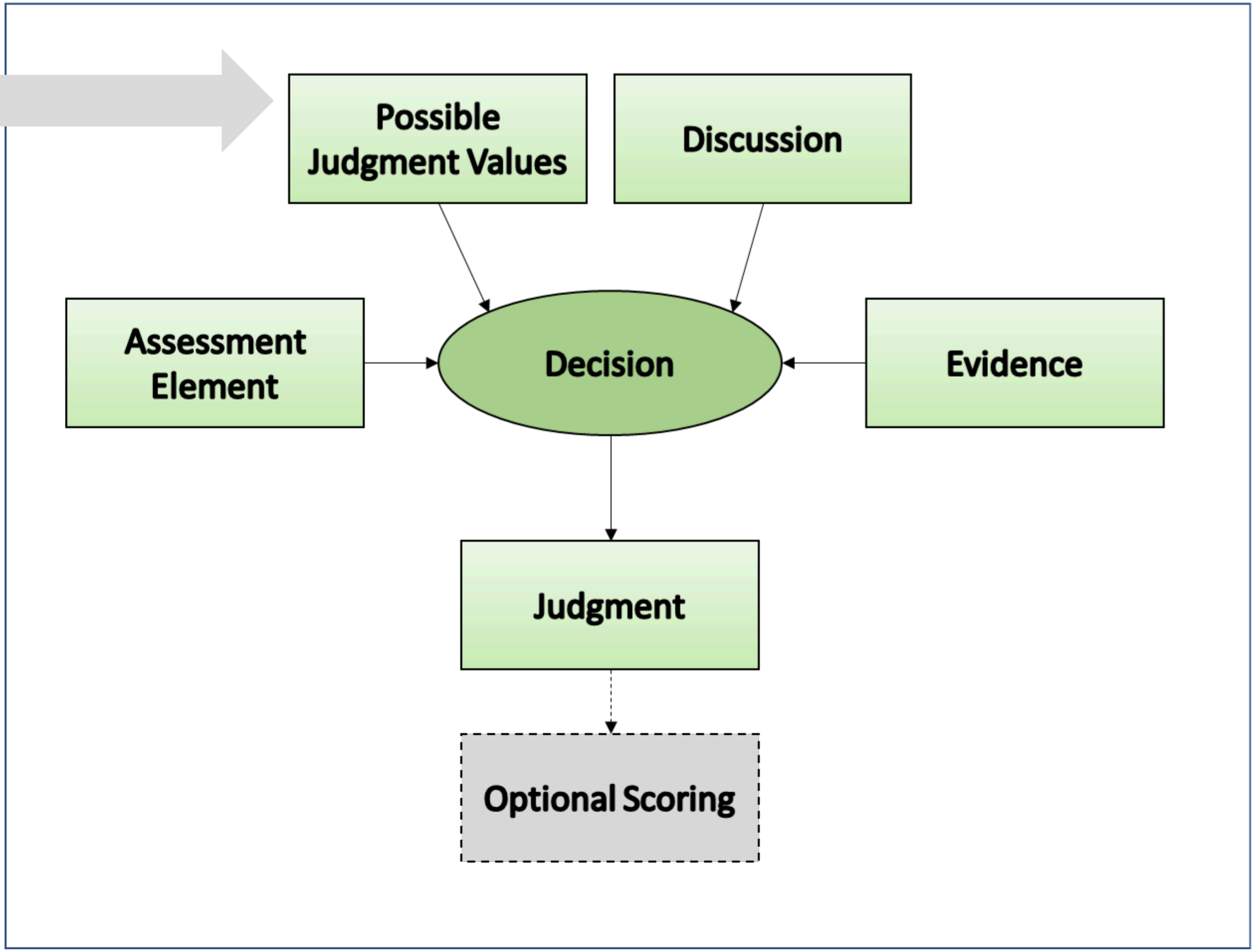
2-043
There is a plan to integrate ISCM into the organization's security culture.

3-044
ISCM is integrated into the organization's security culture.

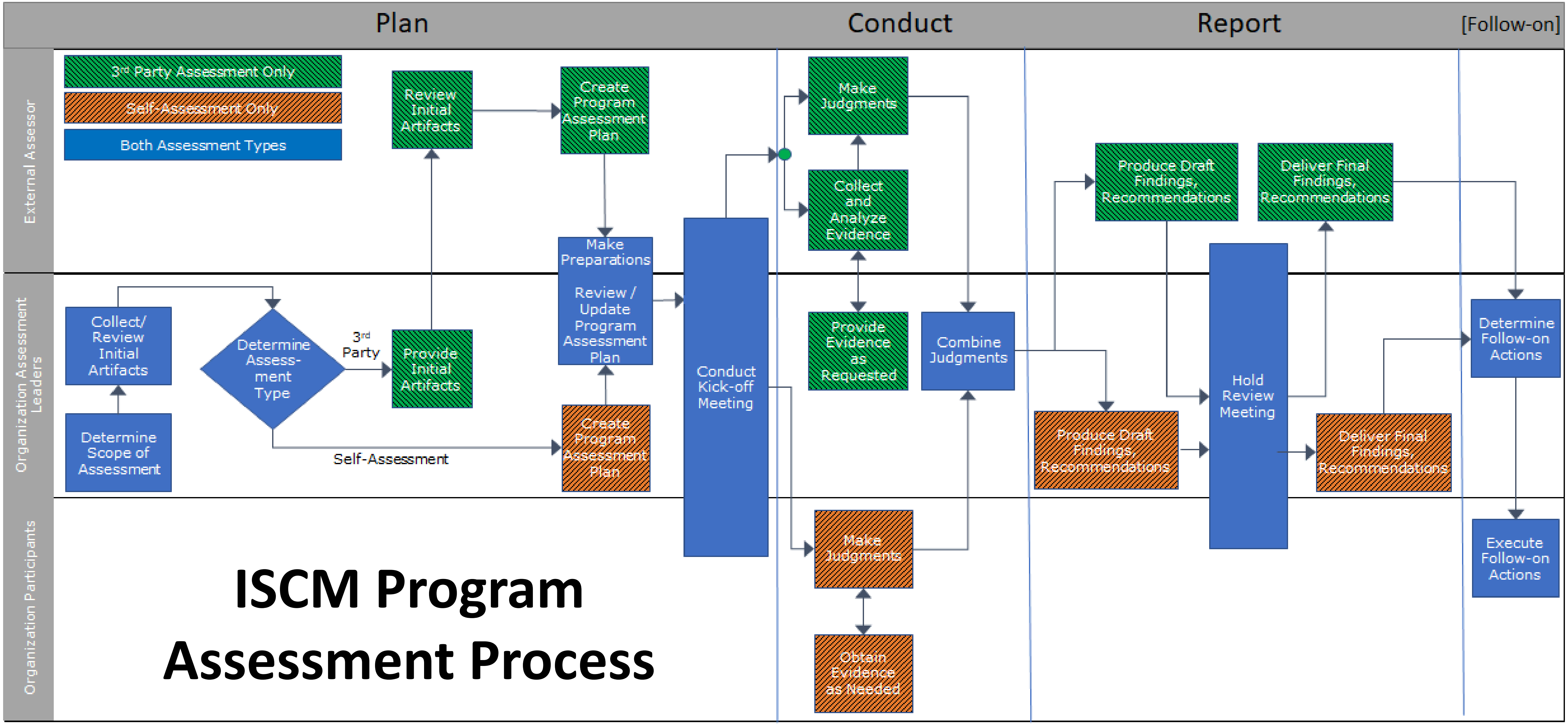
EXAMPLE

# ISCM Judgements

**Satisfied**
Or
**Other than Satisfied**



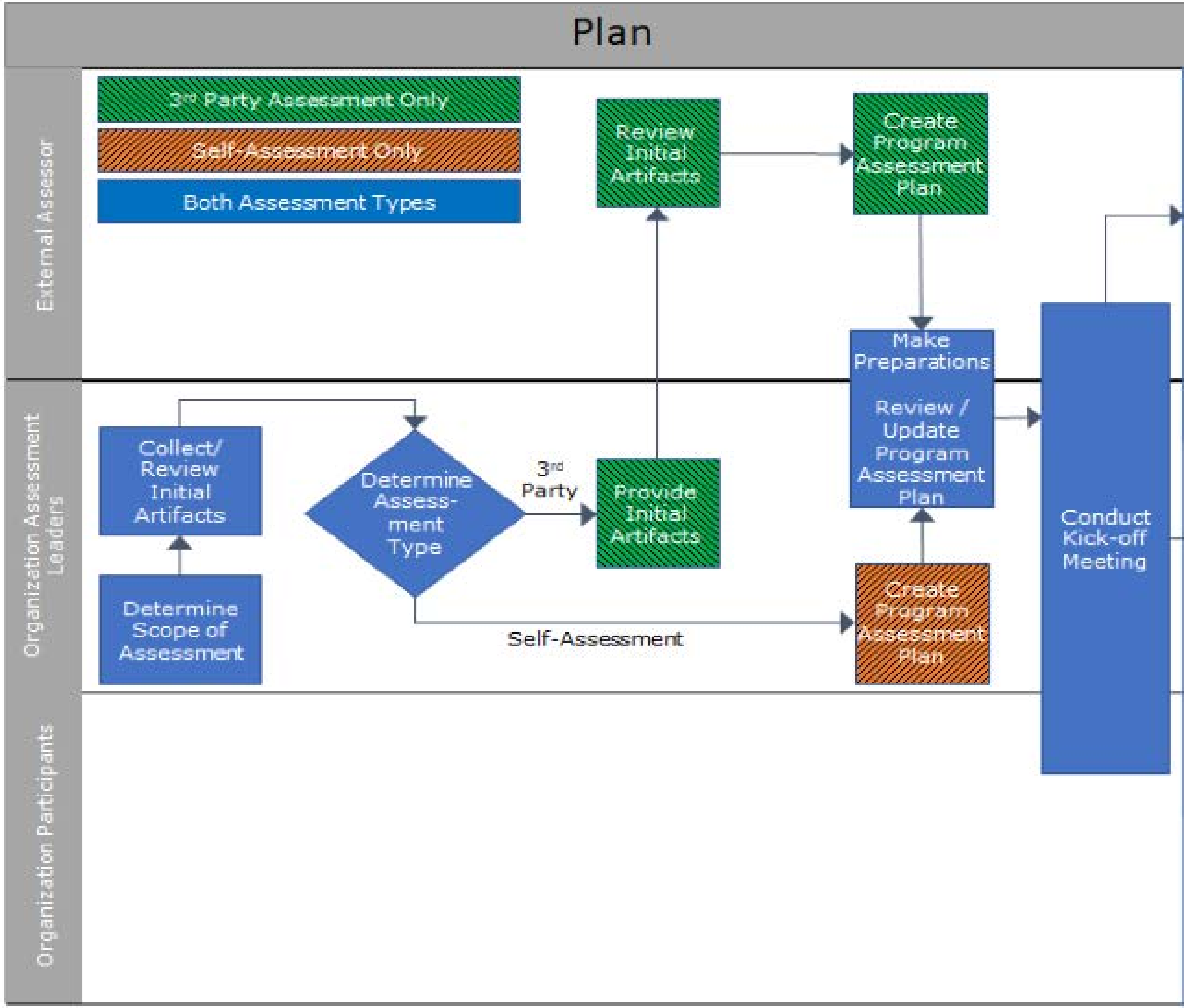
# ISCM Program Assessment Process


Plan
Conduct
Report
[Follow-on]
External Assessor
Organization Assessment Leaders
Organization Participants
3rd Party Assessment Only
Self-Assessment Only
Both Assessment Types
Review Initial Artifacts
Create Program Assessment Plan
Make Preparations
Review / Update Program Assessment Plan
Collect/ Review Initial Artifacts
Determine Scope of Assessment
Determine Assess-ment Type
3rd Party
Provide Initial Artifacts
Self-Assessment
Create Program Assessment Plan
Conduct Kick-off Meeting
Make Judgments
Collect and Analyze Evidence
Provide Evidence as Requested
Combine Judgments
Make Judgments
Obtain Evidence as Needed
Produce Draft Findings, Recommendations
Deliver Final Findings, Recommendations
Hold Review Meeting
Produce Draft Findings, Recommendations
Deliver Final Findings, Recommendations
Determine Follow-on Actions
Execute Follow-on Actions

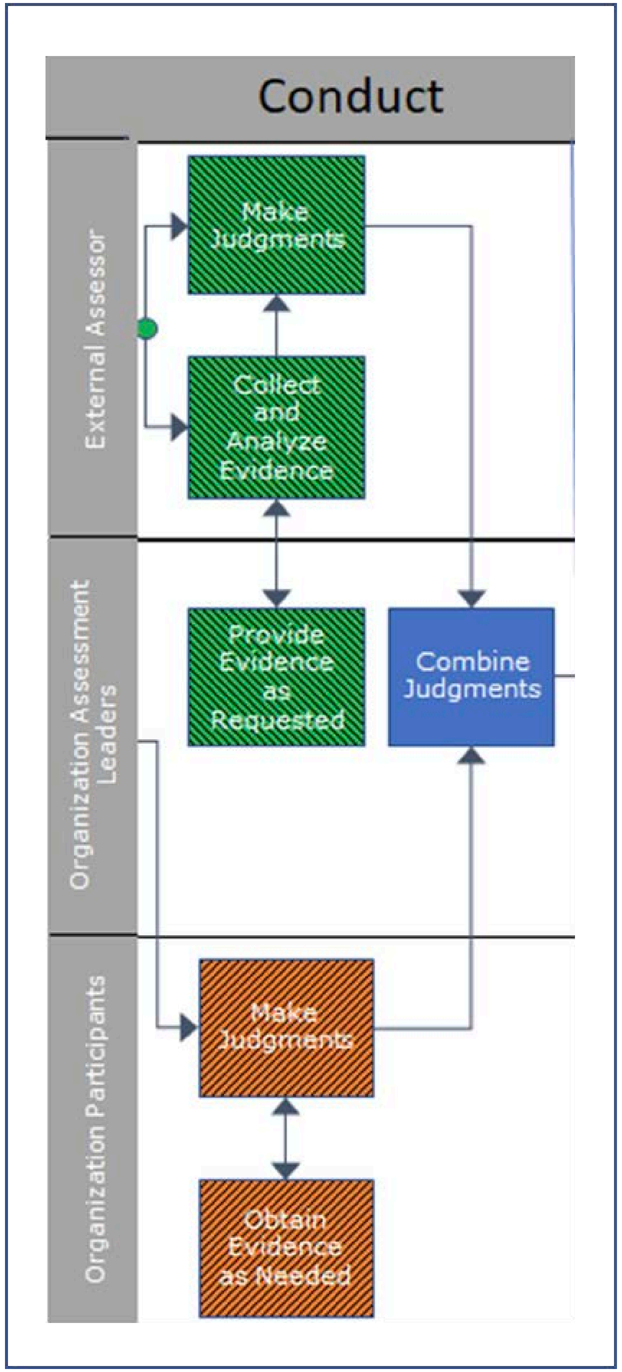
CISA
CYBER+INFRASTRUCTURE

National Institute of Standards and Technology
U.S. Department of Commerce

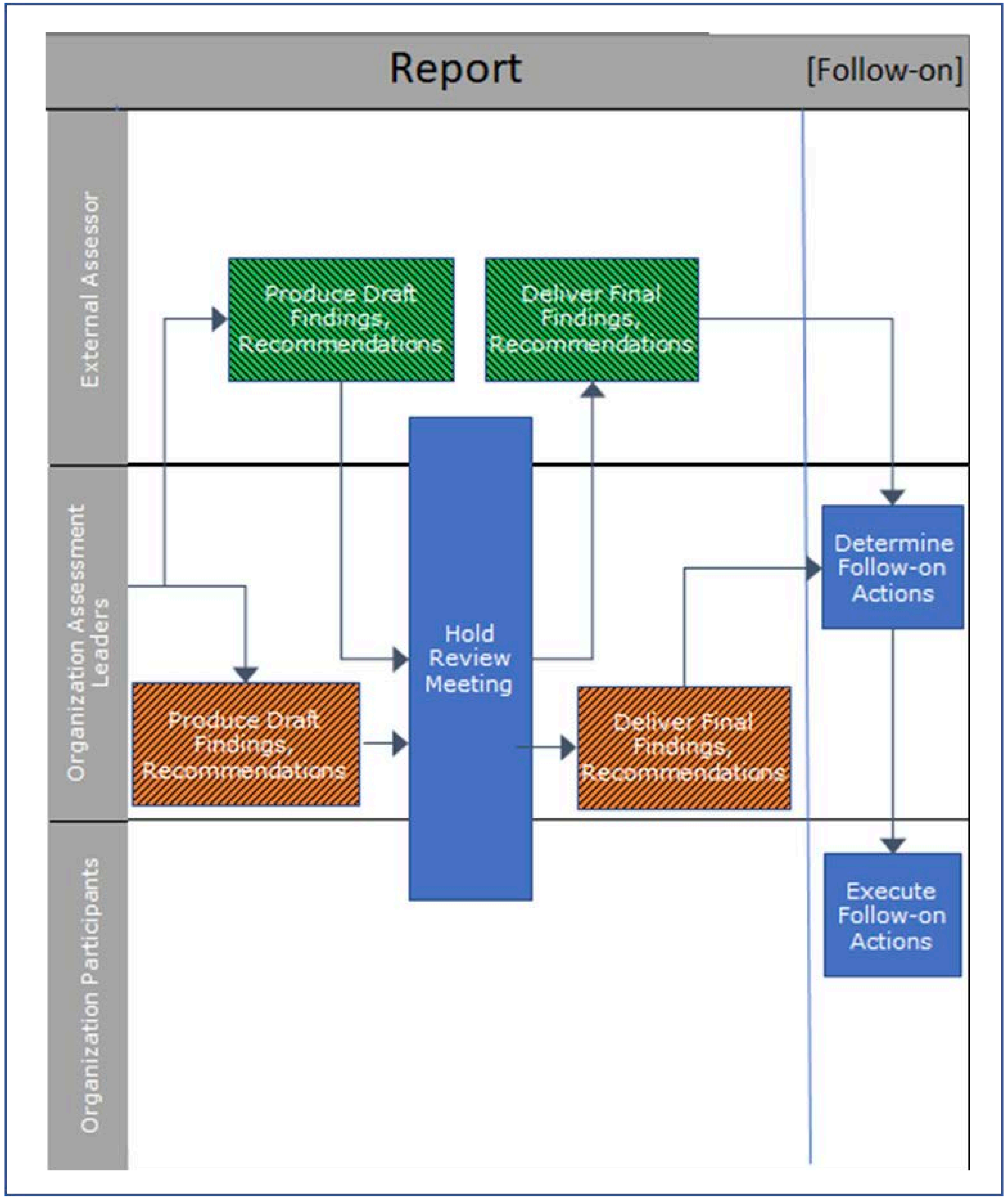
# ISCM Program Assessment Process: **Plan**


Plan
External Assessor
Organization Assessment Leaders
Organization Participants
3rd Party Assessment Only
Self-Assessment Only
Both Assessment Types
Review Initial Artifacts
Create Program Assessment Plan
Make Preparations
Review / Update Program Assessment Plan
Conduct Kick-off Meeting
Collect/ Review Initial Artifacts
Determine Scope of Assessment
Determine Assess-ment Type
3rd Party
Provide Initial Artifacts
Self-Assessment
Create Program Assessment Plan

# ISCM Program Assessment Process: Conduct


Conduct
External Assessor
Make Judgments
Collect and Analyze Evidence
Organization Assessment Leaders
Provide Evidence as Requested
Combine Judgments
Organization Participants
Make Judgments
Obtain Evidence as Needed

# ISCM Program Assessment Process: Report


Report
[Follow-on]
External Assessor
Organization Assessment Leaders
Organization Participants
Produce Draft Findings, Recommendations
Deliver Final Findings, Recommendations
Hold Review Meeting
Produce Draft Findings, Recommendations
Deliver Final Findings, Recommendations
Determine Follow-on Actions
Execute Follow-on Actions

# Next Steps, Q&A and Contact

Draft NIST SP 800-137A public comment open until **February 28, 2020**

Submit comments to sec-cert@nist.gov

Thank you to our co-authors - Kelley Dempsey (NIST), Bob Niemeyer, Ron Rudman and Susan Urban (MITRE)

https://csrc.nist.gov/publications/detail/sp/800-137a/draft

chad.baer@cisa.dhs.gov

victoria.yan@nist.gov

CISA
CYBER+INFRASTRUCTURE

NIST National Institute of Standards and Technology
U.S. Department of Commerce