

Cybersecurity Measurement Workshop



Slack channel: You can join Slack using the invite link in your attendee email or by scanning the QR code.

Submit a question: Type your question in the Q&A box in BlueJeans Events.

Technical support: Send a message using the moderator chat.

Inquiries: cyber-measures@list.nist.gov

Agenda

11:00 AM – 1:30 PM EDT (UTC-4)

| | |
|-----------------|--|
| 11:00 am | Welcome |
| 11:10 am | Panel Discussion with Q&A |
| 12:30 pm | Break |
| 12:40 pm | Overview of 800-55 with Q&A |
| 1:25 pm | Wrap-up |
| 1:30 pm | Adjourn |

Cybersecurity Measurement Workshop

December 13, 2022

Welcome

Charles Romine
Director, Information Technology Lab

Panelists

Khalid Hasan

Allison Krache
Giddens

Matthew Light

Tom Siu

Howard Whyte



Thank you to our panelists

Cybersecurity Measurement Workshop



Slack channel: You can join Slack using the invite link in your attendee email or by scanning the QR code.

Submit a question: Type your question in the Q&A box in BlueJeans Events.

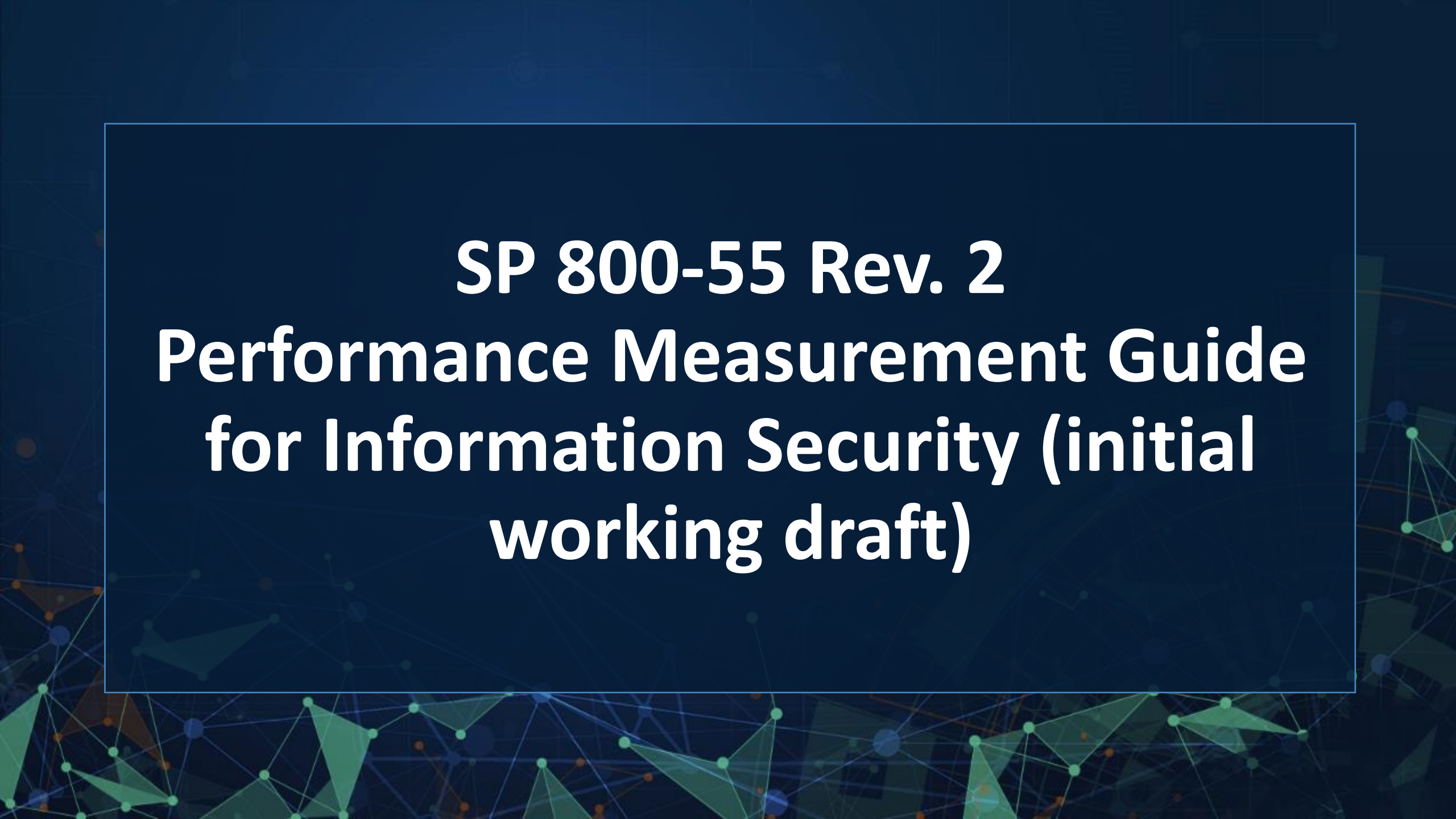
Technical support: Send a message using the moderator chat.

Inquiries: cyber-measures@list.nist.gov

Agenda

11:00 AM – 1:30 PM EDT (UTC-4)

| | |
|-----------------|--|
| 11:00 am | Welcome |
| 11:10 am | Panel Discussion with Q&A |
| 12:30 pm | Break |
| 12:40 pm | Overview of 800-55 with Q&A |
| 1:25 pm | Wrap-up |
| 1:30 pm | Adjourn |

The background of the slide is a dark blue color with a complex network diagram. The diagram consists of numerous small, semi-transparent green and blue polygons connected by thin white lines, creating a web-like structure. The overall aesthetic is technical and modern.

SP 800-55 Rev. 2
Performance Measurement Guide
for Information Security (initial
working draft)

History of the Publication

- SP 800-55, *Security Metrics Guide for Information Technology*
 - August 2003
- SP 800-55 Rev. 1, *Performance Guide for Information Security*
 - July 2008

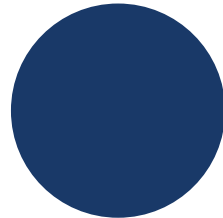
Comment Submission



SP 800-55 Rev. 2 (Draft)

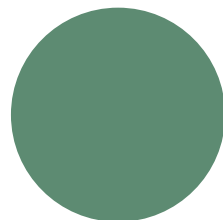
Performance Measurement Guide for Information Security (initial working draft)

Comments Due: February 13,
2023



More information at:

<https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft>



Email Comments to:

cyber-measures@list.nist.gov

Note to Reviewers

Note to Reviewers: We seek to define terms as used in this document. We welcome suggestions of terminology that may need further clarity.

Fundamentals

- Document Conventions
- Benefits of Using Measures
- Critical Success Factors
- Types of Measures
- Measurement Considerations
- Program Scope

Development Process

- Stakeholders and interests
- Goals and objectives
- Policies, guidelines, and procedures
- Program implementation
- Level of implementation
- Program results
- Business/mission impact

Program Implementation

- Prepare for data collection
- Collect and analyze results
- Identify collective actions
- Develop a business case
- Obtain resources
- Apply corrective actions

Goal: Providing a common taxonomy

Terminology

**Benefits of
Using Measures**

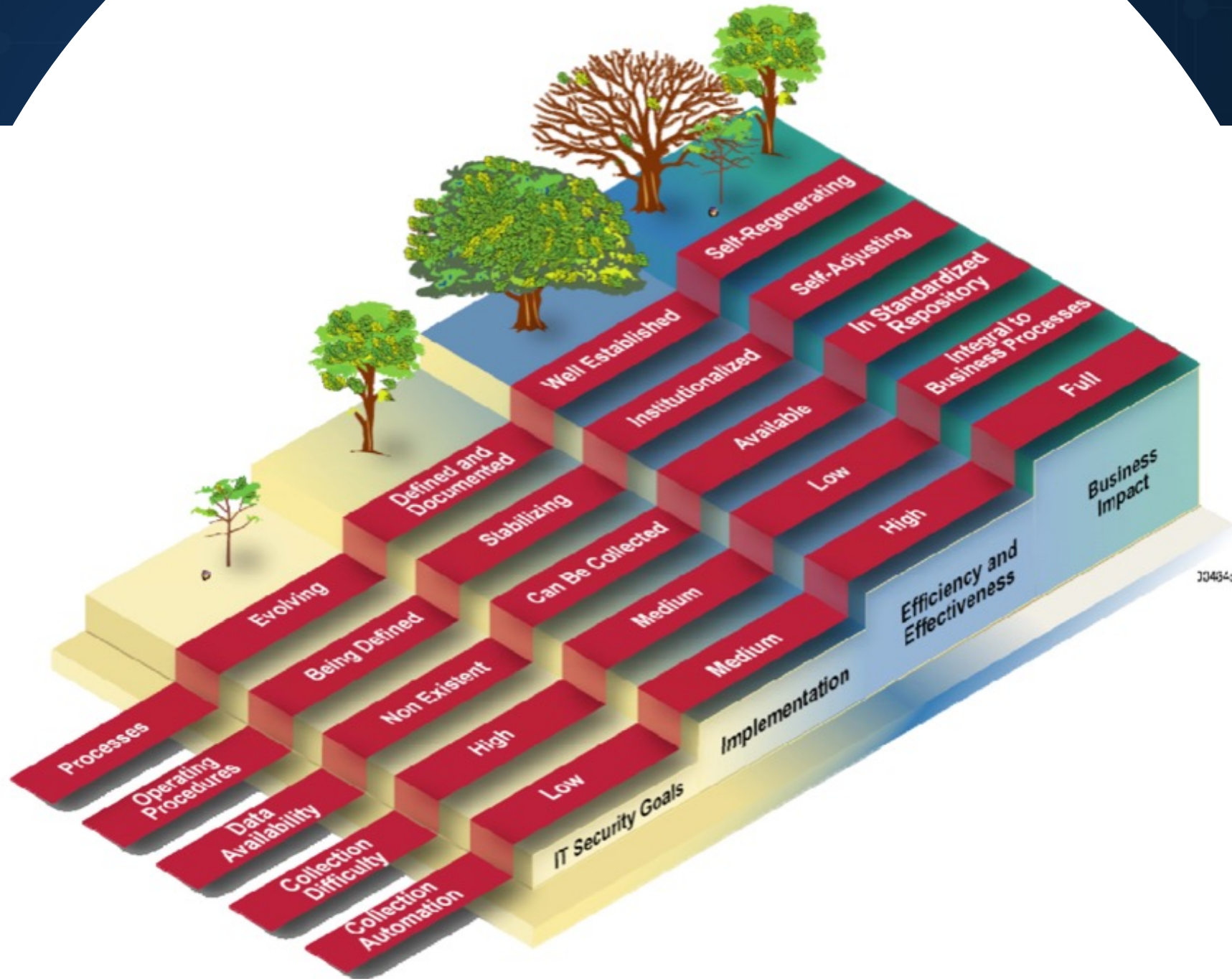
**Critical Success
Factors**

Types of Measures

Implementation

**Efficiency and
Effectiveness**

Business Impact



30454c

Measurement Considerations

- Organizational Considerations
- Manageability
- Data Management Concerns
- Measurement Quality
- Trends and Historical Information
- Automation of Data Collection

Program Scope

- Individual Information Systems
- Enterprise-wide Program

New Content Area: Measurement Quality

- Clearly defined data gathering and reporting requirements
- Standardizing the measurement process
- Ensuring data quality and validity
- Tracking changes over time to ensure consistency
- Repeatability of processes

New Content Area: Trends and Historical Information

- Staying up to date on current rising threats
- Including horizon scanning
- Using the organization's analytic results
- Avoiding recency bias

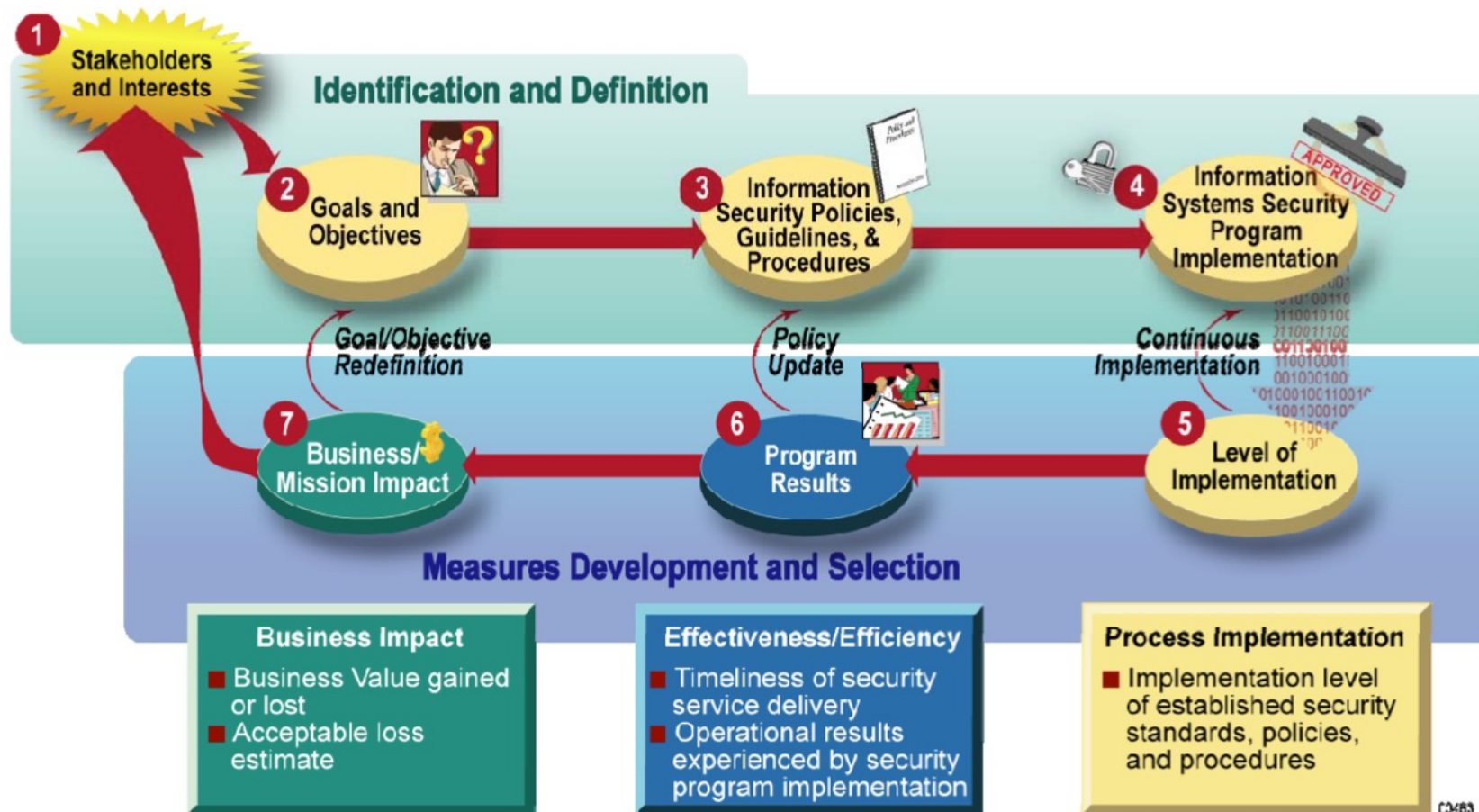
Measurement Considerations

- Organizational Considerations
- Manageability
- Data Management Concerns
- Measurement Quality
- Trends and Historical Information
- Automation of Data Collection

Program Scope

- Individual Information Systems
- Enterprise-wide Program

Measures Development Process



**Stakeholder
Identification**

**Goals and
Objectives**

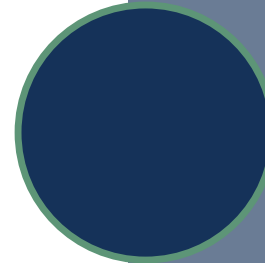
New Content Area: Governance and Compliance

- Governance structures
- Laws and regulations
- Industry guidance
- Various outside requirements

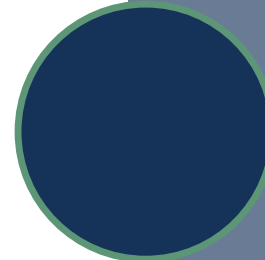
**Policies, Guidelines,
and Procedures
Review**

**Measurement
Program
Implementation**

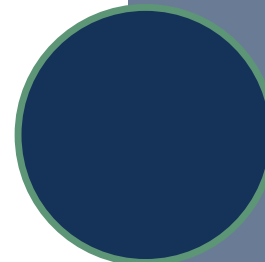
Measures Development and Selection



Level of
Implementation



Program Results



Business/Mission
Impact

New Content Area: Measures Prioritization and Selection

- Risk-based approach
- Effective use of data
- Measuring existing and established processes

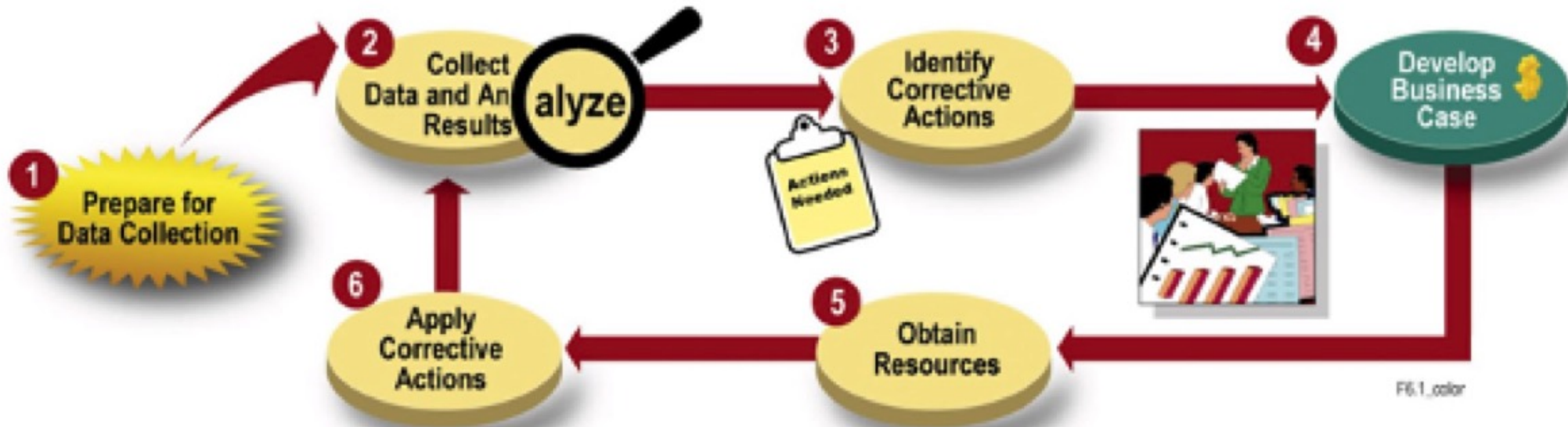
New Content Area: Defining Evaluation Methods

- Assessing against baselines and acceptable ranges
- Component testing
- Monitoring for anomalies
- Success hitting control targets
- Indicators
- Frameworks
- Maturity Modeling
- Compliance

**Measures
Development
Template**

**Feedback within
Development
Process**

Measures Program Implementation



Phase 1: Prepare for Data Collection

Phase 2:
Collect Data and Analyze Results

New Content Area: Data Collecting and Reporting

- Automated data collection and reporting
- Manual data collecting and reporting

Phase 3: Identify Corrective Actions

Phases 4 and 5: Develop and Business Case Obtain Resources

Phase 6: Apply Corrective Actions



Next Steps



Questions?

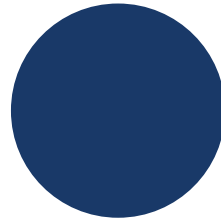
Comment Submission



SP 800-55 Rev. 2 (Draft)

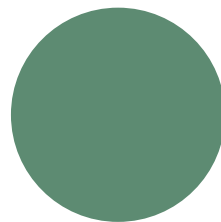
Performance Measurement Guide for Information Security (initial working draft)

Comments Due: February 13,
2023



More information at:

<https://csrc.nist.gov/publications/detail/sp/800-55/rev-2/draft>



Email Comments to:

cyber-measures@list.nist.gov

STAY IN TOUCH

CONTACT US



NIST.gov



@nist