Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been followed by the document identified below.

Withdrawal Date January 17, 2024

Original Release Date November 14, 2022

The attached draft document is followed by:

Status Initial Public Draft (ipd)

Series/Number NIST SP 800-55v1 ipd; NIST SP 800-55v2 ipd

Title Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures

Measurement Guide for Information Security: Volume 2 — Developing an Information Security Measurement Program

Publication Date January 2024

DOI https://doi.org/10.6028/NIST.SP.800-55v1.ipd

https://doi.org/10.6028/NIST.SP.800-55v2.ipd

CSRC URL https://csrc.nist.gov/pubs/sp/800/55/v1/ipd

https://csrc.nist.gov/pubs/sp/800/55/v2/ipd

Additional Information

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-55r2 iwd

Performance Measurement Guide for Information Security

Initial Working Draft

Katherine Schroeder
Hung Trinh

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-55r2.iwd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-55r2 iwd

Performance Measurement Guide for Information Security

Initial Working Draft

Katherine Schroeder
Hung Trinh
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-55r2.iwd

December 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Working Draft

This is a Working Draft (WD). It is not yet complete, and organizations should not attempt to implement it. The content is in an early stage of development and has not been extensively edited or vetted. This provides an insider view of the development of the content and gives NIST an opportunity to share early thoughts, ideas, and approaches with stakeholders. NIST welcomes early informal feedback and comments, which will be adjudicated after the specified public comment period. Before final publication, there will be at least one complete "initial public draft" posted for public comment.

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Fair Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [will be added upon final publication]
Supersedes NIST Series XXX (Month Year) DOI [will be added upon final publication]

How to Cite this NIST Technical Series Publication:
Schroeder K, Trinh H (2022) Performance Measurement Guide for Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-55r2 iwd. https://doi.org/10.6028/NIST.SP.800-55r2.iwd

Author ORCID iDs
Author 1: 0000-0000-0000-0000 [will be added upon final publication]
Author 2: 0000-0000-0000-0000

Public Comment Period
November 14, 2022 – February 13, 2023

Submit Comments
cyber-measures@list.nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This document provides guidance on how an organization can use metrics to identifies the adequacy of an in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments. The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports.

Keywords

information security; metrics; measures; security controls; performance; reports.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Note to Reviewers

We seek input on the changes being proposed to SP 800-55. New sections are noted as new additions to SP 800-55. Many are also marked by a "Note to Reviewer" with a request for feedback. These questions are meant to facilitate discussion and should not discourage input on any other topics within this annotated outline. There are three additional questions for reviewer consideration. These questions are:

1) CIOs and CISOs: What measurement and metrics guidance would benefit your program?
2) How to best communicate information security measurement needs up and down the organizational structure?
3) Examples: What kinds of measures and metrics examples or templates could this publication provide that would be helpful in your work?

This working draft also has sections with only minor planned changes marked as "intentionally left out of this review cycle" to allow for readers to focus on the more substantial proposed changes. The Initial Public Draft will include the full proposed text for all sections of the

document. Feedback is still welcome on the sections not highlighted in this Initial Working Draft.

A virtual public forum will be held on December 13, 2022, to introduce the working draft of SP 800-55 and highlight the various questions for reviewers within the document through a panel of practitioners across different sectors.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: cyber-measures@list.nist.gov, with the subject "NIST SP 800-55r2 call for patent claims"

156 **Table of Contents**

Note to Reviewers: We seek input on the changes being proposed to SP 800-55. New sections are noted as new additions to SP 800-55. Many are also marked by a "Note to Reviewer" with a request for feedback. These questions are meant to facilitate discussion and shouldn't discourage input on any other topics within this annotated outline. In addition, there are two additional questions that are asking for reviewer consideration. These questions will be addressed in a public forum on December 13, 2022. These questions are:

CIOs and CISOs: What measurement and metrics guidance would benefit your program?

How to best communicate information security measurement needs up and down the organizational structure?

Examples: What kinds of measures examples and templates could we provide that would be helpful in your work?

1. Introduction

1.1. Purpose and Scope

This section only has minor updates from [1.1 Purpose and Scope] in the current [SP800-55] and is intentionally left out of this review cycle

Summary: NIST Special Publication (SP) 800-55, Revision 2 is a guide to the development, selection, and implementation of information security measures. It is intended to provide an infrastructure for data collection, analysis, and reporting that can be tailored to support regulatory requirements and organizational needs.

Any additional input on this section is welcome.

1.2. Audience

This section only has minor updates from [1.2 Audience] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: This guide is written primarily for Chief Information Officers, Chief Information Security Officers, and others who work closely with measurement and metrics programs within industry and government.

Any additional input on this section is welcome.

1.3. Relation to Other NIST Publications

This section only has minor updates from [1.3 Relation to Other NIST Publications] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: This document is intended to provide considerations for measurement of the information security program activities described in several NIST publications, including:

- *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST Cybersecurity Framework) [CSF]
- NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Security Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [SP800-37]
- NIST SP 800-161r1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* [SP800-161]
- NIST Internal Report (IR) 8286, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)* [IR8286]

Any additional input on this section is welcome.

1.4. Document Organization

This section only has minor updates from [1.6 Document Organization] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: The remaining sections of this document discuss the following:

- Chapter 2, Information Security Measures and Fundamentals
- Chapter 3, Measurement Program Development Process
- Chapter 4, Information Security Measurement Program Implementation

Any additional input on this section is welcome.

2. Information Security Measures Fundamentals

2.1. Document Conventions

2.1.1. Terminology

This section is a new addition to [SP800-55] and will establish how words will be used within the document

- Information security: The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. [FIPS200]
- Measurement: The process of experimentally obtaining one or more quantity values that can be reasonably attributed to a quantity. [MetricsMeasures]
- Measures: An objective and concrete attribute. Should be quantifiable and observable. Used as the basis for metrics. [MetricsMeasures]
- Metrics: Tools designed to facilitate decision-making and improve performance and accountability through collecting, analyzing, and reporting relevant performance-related data. More abstract, higher-level, or subjective than measures. [MetricsMeasures]
- Quantitative Assessment: Use a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment. [SP800-30]
- Qualitative: Use of a set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels. [SP800-30]
- Semi-Quantitative: Use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. [SP800-30]

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

Any additional input on this section is welcome.

2.1.2. Definition

This section only has minor updates from [3.1 Definition] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Information security measures facilitate decision making and improve performance and accountability through collection, analysis, and reporting relevant performance-related data. The purpose of measure performance is to monitor the status of measured activities and facilitate improvement by applying corrective actions based on observable measurements. Measures should be:

- Possible to obtain at different levels within an organization
- Based on information security performance goals and objectives
- Information security measures monitor the accomplishment of goals and objectives by quantifying the implementation, efficiency, and effectiveness of security controls.
- Data required for calculating measures must be readily obtainable, and the process under consideration needs to be measurable.
- Allow for tracking performance and directing resources.

Any additional input on this section is welcome.

2.2. Benefits of Using Measures

This section only has minor updates from [3.2 Benefits of Using Measures] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: An information security measurement program provides several organizational and financial benefits:

- Increase Accountability
- Improve Information Security Effectiveness
- Demonstrate Compliance
- Provide Quantifiable Inputs for Resource Allocation Decisions

New Additions:

- Manage Risk
- Continuous Analysis

Any additional input on this section is welcome.

2.3. Critical Success Factors

This section only has minor updates from [1.4 Critical Success Factors] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: An information security measurement program within an organization should include four interdependent components:

- Foundation of strong upper-level management support
- Practical information security policies & procedures
- Quantifiable performance measures
- Results-oriented measures and analysis

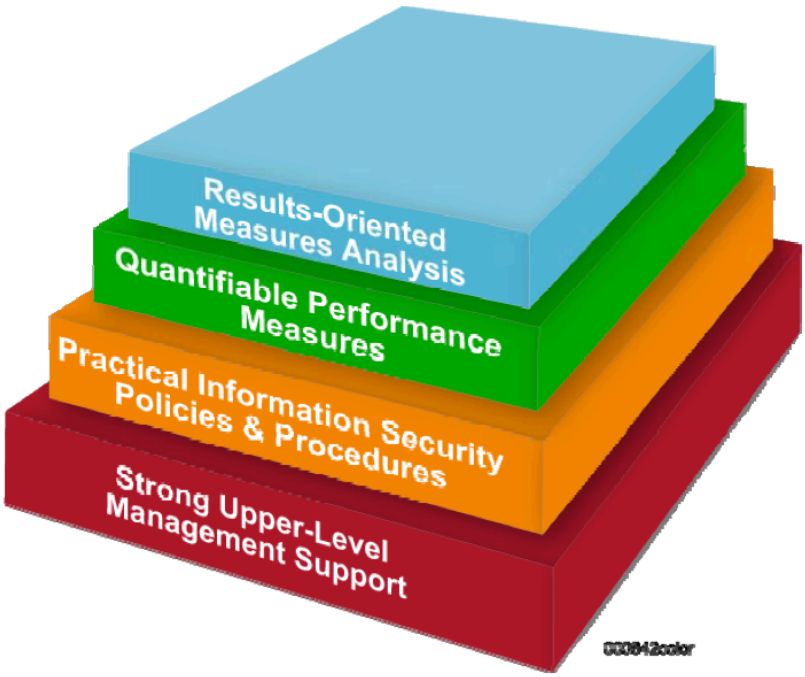

Fig. 1. Information Security Measurement Program Structure

Any additional input on this section is welcome.

2.4. Types of Measures

This section only has minor updates from [3.3 Types of Measures] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Organizational maturity determines the types of measures an organization can gather successfully. The existence and institutionalization of processes and procedures define this maturity. This section explores types of measures – implementation, effectiveness/efficiency, and business impact – against the measurement of processes, operating procedures, data availability, collection difficulty, collection automation.

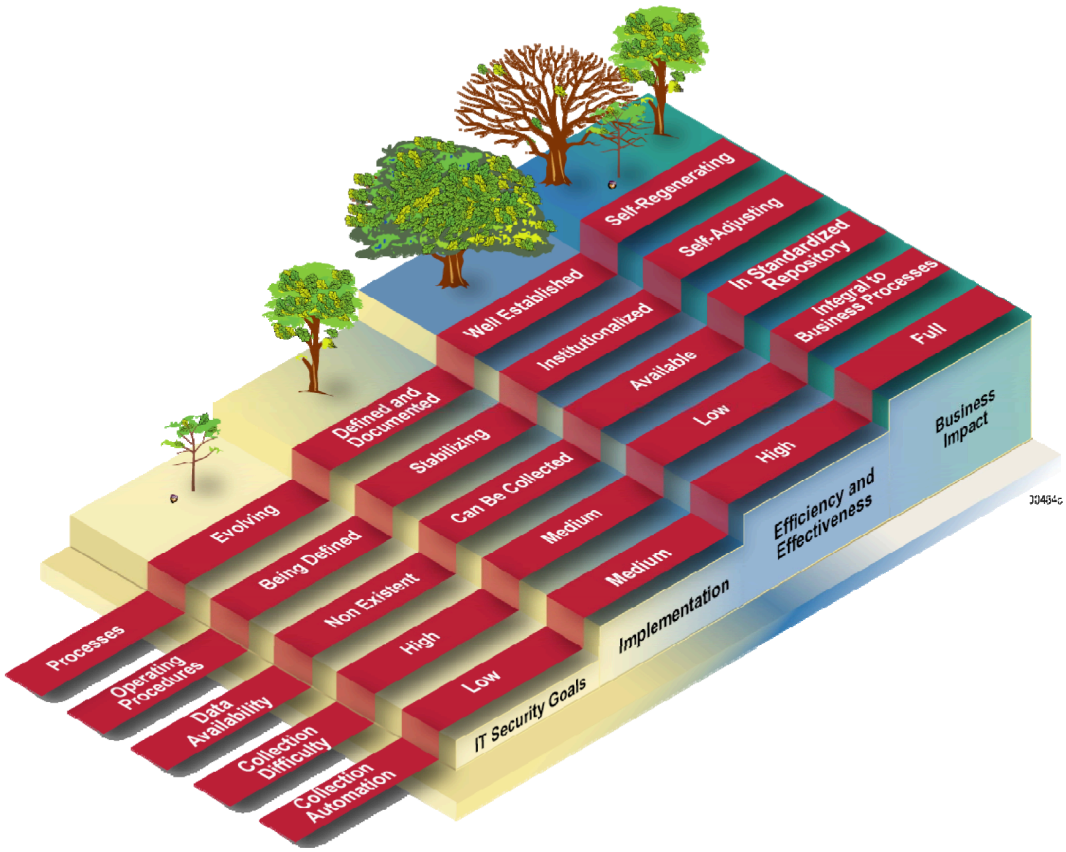

Fig. 2. Information Security Program Maturity and Types of Measurement

Any additional input on this section is welcome.

2.4.1. Implementation Measures

> *This section only has minor updates from [3.3.1 Implementation Measures] in the current [SP800-55] and is intentionally left out of this review cycle.*

Summary: Implementation measures demonstrate progress in implementing information security programs, specific security controls, and associated policies and procedures. Implementation measures can also examine system-level areas. These measures require data obtained using common means of documenting and tracking information security program activities.

Any additional input on this section is welcome.

2.4.2. Effectiveness/Efficiency Measures

This section only has minor updates from [3.3.2 Effectiveness/Efficiency Measures] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Effectiveness/Efficiency measures are used to monitor if program-level processes and system- level security controls are implemented correctly, operating as intended, and meeting the desired outcome. These measures concentrate on the evidence and results of assessments and may require multiple data points quantifying the degree to which information security controls are implemented and the resulting effect(s) on the organization's information security posture. Effectiveness/efficiency measures address two aspects of security control implementation results: the robustness of the result itself, referred to as ***effectiveness***, and the timeliness of the result, referred to as ***efficiency.***

Any additional input on this section is welcome.

2.4.3. Impact Measures

This section only has minor updates from [3.3.3 Impact Measures] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Impact measures articulate the impact of information security on an organization's mission. These measures are inherently organization-specific and combine information about the results of security controls implementation with information about resources. Resource information across an organization is tied directly to information security activity and events that must be tracked to assess impact measures.

Any additional input on this section is welcome.

2.5. Measurement Considerations

This section only has minor updates from [3.4 Measurement Considerations] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Organizations embarking on information security performance measurement should be aware of several considerations for helping their program succeed. These include specific organizational structures and processes. Successful information security performance measurement also requires understanding budget, personnel, and time resources.

Any additional input on this section is welcome.

2.5.1. Organizational Considerations

This section only has minor updates from [3.4.1 Organizational Considerations] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: The development of information security metrics and program implementation requires the involvement of appropriate stakeholders across various organizational elements that interact with information security. Each stakeholder should provide inputs to the measures development effort to ensure that the collected measures are meaningful yield impact and outcome findings and provide results necessary to address performance gaps.

Any additional input on this section is welcome.

2.5.2. Manageability

This section only has minor updates from [3.4.2 Manageability] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Any information security measurement program must be manageable for the implementing organization. As resources are limited organizations should prioritize measurement requirements to ensure that a limited number of measures are gathered. As the program matures and target levels of measurement are reached, obsolete measures should be phased out and new ones that measure completion and effectiveness of more current items should be used.

Any additional input on this section is welcome.

2.5.3. Data Management Concerns

This section only has minor updates from [3.4.3 Data Management Concerns] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: To ensure the quality and validity of data, data collection methods and data repositories used for measures data should be standardized. Although substantial amounts of data may be collected, not all data will be useful for an information security measurement program and any given point in time. Data collection should be as nonintrusive as possible. The operational and vulnerability information contained in information security data repositories needs to be protected appropriately due to the sensitive nature of the data.

Any additional input on this section is welcome.

2.5.4. Measurement Quality

This section is a new addition to [SP800-55] and will discuss areas of focus within measurement quality. These include:

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

Note to Reviewers: Are there other areas of focus you would like to see represented when examining quality of measurement?

Any additional input on this section is welcome.

2.5.5. Trends and Historical Information

This section is a new addition to [SP800-55] and will explore how trends and historical data impact the allocation of resources. Areas of focus include:

- Staying up to date on current rising threats to include as part of a continuous measurement process.
- Including horizon scanning exercises to increase system resilience
- Using the organization's analytic results about event probability
- Avoiding recency bias about current events when determining courses of action and resource allocation.

Any additional input on this section is welcome.

2.5.6. Automation of Data Collection

This section only has minor updates from [3.4.4 Automation of Data Collection] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Efficient data management is facilitated by automating measurement data collection. Automating measurement data collection standardizes data collection and reporting and helps institutionalize measurement activity by integrating it into business processes. In addition, automated data collection minimizes opportunities for human error, leading to greater accuracy of available data.

Any additional input on this section is welcome.

2.6. Information Security Measurement Program Scope

This section only has minor updates from [3.5 Information Security Measurement Program Scope] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: An information security measurement program can be scoped to a variety of environments and needs, such as quantifying system-level and enterprise-wide information security performance. Information security measures can be applied to organizational units, sites, or other organizational constructs. Organizations should be carefully defining the scope of their information security measurement program based on specific stakeholder needs, strategic goals and objectives, operating environments, risk priorities, and information security program maturity.

Any additional input on this section is welcome.

2.6.1. System Level

This section only has minor updates from [3.5.1 Individual Information Systems] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Information security measurement can be applied at the system level to provide quantifiable data regarding the implementation, effectiveness/efficiency, or impact of required or desired security controls. Information security measurement can support certification and accreditation, FISMA reporting, or capital planning activities. Any additional input on this section is welcome.

2.6.2. Enterprise-wide Program

This section only has minor updates from [3.5.3 Enterprise-Wide Program] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Information security measurement can be implemented on an enterprise-wide level to monitor an organization's information security activities. Enterprise-level measures can be derived by aggregating multiple system-level measures or developed by using the entire enterprise as the scope. These aggregated and individual information security measurements are then used to inform decisions made on an enterprise level.

Any additional input on this section is welcome.

3. Measures Development Process

This section only has minor updates from [5. Measures Development Process] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Overview of considerations when selecting appropriate measures for an organization to pursue. This illustrates an iterative process with two major activities:

- Identify and define the current information security measurement program
- Develop and select specific measures to gauge the implementation, effectiveness/efficiency, and impact of the organization's security controls.

This development process is a way to think about measures and identify measures tailored to organizational needs, not as a sequential guide. The information security measure development process includes seven phases:

1. Stakeholders and interests
2. Goals and objectives
3. Information security policies, guidelines, and procedures
4. Information security program implementation
5. Level of implementation
6. Program results
7. Business/mission impact

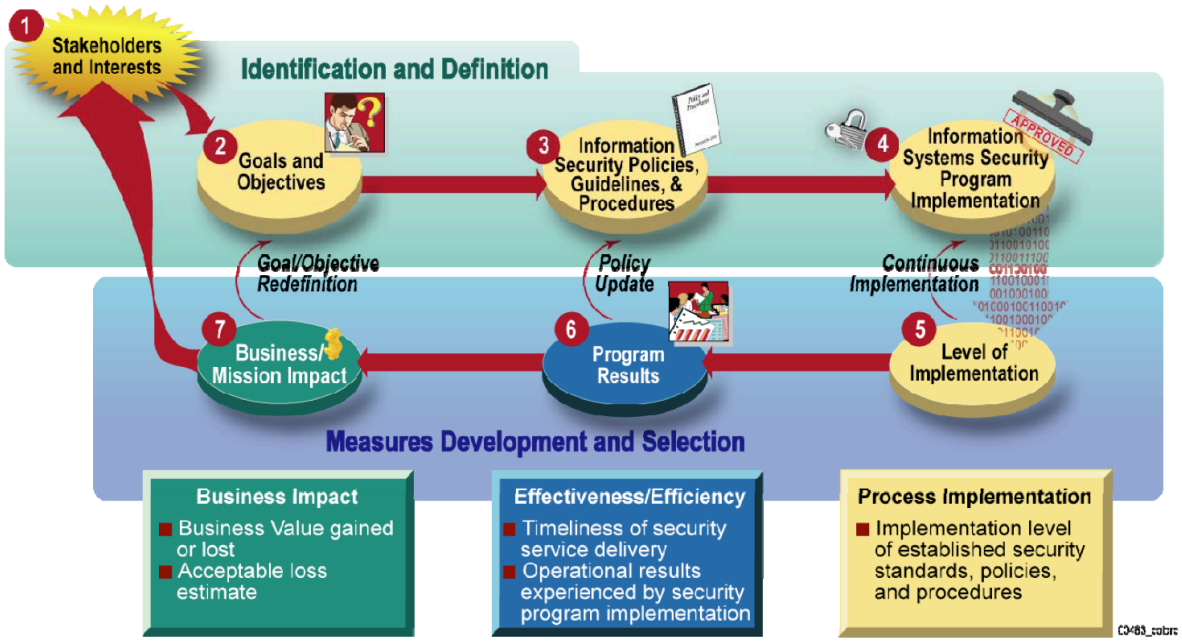

Fig. 3. Information Security Measurement Development Process

Any additional input on this section is welcome.

3.1. Stakeholder Identification

This section only has minor updates from [5.1 Stakeholder Identification] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Phase 1 is identifying relevant stakeholders. Stakeholder interests will differ depending on their roles and position within the organization. Each stakeholder may require an additional set of customized measures that give insight into their area of responsibility.

Any additional input on this section is welcome.

3.2. Goals and Objective Definition

This section only has minor updates from [5.2 Goals and Objective Definition] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Phase 2 is identifying and documenting information security program goals and objectives that would guide security control implementation. Information security program goals can also be derived from enterprise-level goals and objectives in support of the overall organization's mission.

Any additional input on this section is welcome.

3.2.1. Governance and Compliance

This section is a new addition to [SP800-55] and will explore how goals and objectives may be determined by goals created outside of the information security program, including:

- Governance structures
- Laws and regulations
- Industry guidance
- Various requirements from outside the organizational structure, such as:
    - Insurance
    - Auditors
    - Accreditation bodies
    - Compliance reviews

Note to Reviewers: We seek input on how organizations address and balance goals and objectives required by outside entities as opposed to internal information security program goals and objectives.

Any additional input on this section is welcome.

3.3. Information Security Policies, Guidelines, and Procedures Review

This section only has minor updates from [5.3 Information Security Policies, Guidelines, and Procedures Review] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Phase 3 focuses on reviewing organization-specific security practices that define a baseline for information security practices. These policies, guidelines, and procedures should be reviewed during the measures development process and periodically afterward.

Any additional input on this section is welcome.

3.4. Information Security Measurement Program Implementation Review

This section only has minor updates from [5.4 Information Security Program Implementation Review] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Phase 4 consists of reviewing any existing measures or data repositories that could be used to derive measures. The retirement of existing measures and development of new measures will continue as the information security measures program evolves.

Any additional input on this section is welcome.

3.5. Measures Development and Selection

This section only has minor updates from [5.5 Measures Development and Selection] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Phase 5, 6, and 7 involves developing measures that track the implementation, efficiency/effectiveness, and business impact of an information security program.

Any additional input on this section is welcome.

3.5.1. Measures Development Approach

This section only has minor updates from [5.5.1 Measures Development Approach] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: The scope of the measurement effort informs if the development of information security measures should focus on gauging the security performance of a specific security control, a group of security controls, or a security program.

Any additional input on this section is welcome.

3.5.2. Measures Prioritization and Selection

This section has significant updates from [5.5.2 Measures Prioritization and Selection] in the current [SP800-55].

There is a huge number of possible measures for an organization to monitor. Measures prioritization ensures that the set selected for initial implementation has the following qualities:

- Facilitates improvement of high priority security control implementation as selected using a risk-based approach
- Uses data from existing sources and data repositories
- Measures existing and established processes
    - Inconsistent processes will not provide meaningful data about information security performance, but measurements may still be used to establish a baseline for continuous monitoring purposes

At this point in the process, a weighing scale may be used to assign values to each measure. Organizations should use a weighing scale that fits their needs while ensuring consistency across the process. The process of developing a weighing scale may utilize the following techniques:

- Event Probability
    - Setting baselines
    - Leverage in-house knowledge and data about existing systems.
    - Organizational assessments, audits, interviews, surveys, and studies are all options.
    - Convert qualitative metrics to quantitative metrics.
    - Examine external data and knowledge.
    - Use raw data to augment existing measurements or to achieve targeted knowledge/metrics.
- Event Probability Models
    - Decomposition theorems for probability density
    - Bayesian methods for probability analysis
    - Binomial distribution, Poisson distribution and Monte Carlo for performance metrics and propagating uncertainty

574 - Copula methods for correlation between risks
575 - Event Tree analysis
576 - Machine learning and predictive models
577 • Consequences
578 - Establish a consequence model by looking at potential events and their outcomes.
579 - Outliers and unexampled events may come up over time. An organization can
580 prepare for these issues using horizon scanning, stress tests, and system resilience.
581 • Consequence Modeling
582 - Expected shortfall
583 - Value at risk – statistical analysis of historical market trends
584 - If a consequence model has already been determined as part of a risk management
585 strategy, the organization should leverage that research.

Note to Reviewers: We seek reviewer input on the prioritization, selection, modeling, and weighing of measures.

586

587 Any additional input on this section is welcome.

588 3.5.3. Establishing Performance Targets

589 *This section only has minor updates from [5.5.2 Establishing*
590 *Performance Targets] in the current [SP800-55] and is intentionally left*
591 *out of this review cycle.*

592 Performance targets establish a benchmark by which success is measured. Implementation
593 measures targets are set for 100 percent completion of assigned tasks. However,
594 effectiveness/efficiency and impact measures will require qualitative and subjective reasoning to
595 determine appropriate and acceptable performance levels. Performance targets and risk tolerance
596 should be determined by upper-level management or even at the board level. These targets and
597 benchmarks require periodic reexamination to ensure appropriate target levels.

598 Any additional input on this section is welcome.

599 3.6. Defining Evaluation Methods

600 *This section is a new addition to [SP800-55] and will look at evaluation*
601 *methods for measuring effectiveness, efficiency, and the impact of risk*
602 *reduction. The focus will be on observable functionalities and outcomes*:

603 • Assessing against baselines and acceptable ranges
604 • Component testing [SP800-84]
605 • Monitoring for anomalies

- Success hitting control targets
- Indicators
  - Key performance indicators
  - Key goal indicators
  - Key risk indicators
  - Critical success factors
  - Leading and lagging indicators
- False positive report rate
- Incident response volume
- Frameworks
- Maturity modeling
- Compliance
- Audits
- Penetration testing
- Bug bounties

The focus of establishing, maintaining, and updating performance targets is on observable functionalities and controls.

Note to Reviewers: We seek reviewer input on additional functionalities, controls, or indicators that could be represented here.

Any additional input on this section is welcome.

3.7. Measures Development Template

This section only has minor updates from [5.6 Measures Development Template] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Organizations should document their performance measures in a standard format to ensure repeatability of measures development, tailoring, collection, and reporting activities. While this section provides a suggested approach for measurement, organizations may prefer to tailor their performance measurement template based on their own needs. Fields of reporting may include:

- Measure ID
- Goal
- Measure
- Type
- Formula
- Target

- Implementation evidence
- Frequency
- Responsible parties
- Data source
- Reporting format

Any additional input on this section is welcome.

3.8. Feedback Within the Development Process

This section only has minor updates from [5.7 Feedback Within the Development Process] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Measures that are ultimately selected for implementation will be useful for:

- Measuring performance
- Identifying causes of unsatisfactory performance
- Pinpointing improvement areas
- Facilitating consistent policy implementation
- Effecting security policy changes
- Redefining goals and objectives
- Supporting continuous improvement

These are shown as the feedback arrows in Figure 3-1 as goal/objective redefinition, policy update, and continuous improvement.

Any additional input on this section is welcome.

4. Information Security Measurement Program Implementation

This section only has minor updates from [6. Information Security Measurement Implementation] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Information security measurement implementation involves applying measures for monitoring information security control performance and using the results to initiate performance improvement actions. The information security measurement program implementation process consists of six phases that – when fully executed – will ensure the continued use of these measures for security control performance monitoring and improvement.

Fig. 4. Information Security Measurement Program Implementation Process

Any additional input on this section is welcome.

4.1. Prepare for Data Collection

This section only has minor updates from [6.1 Prepare for Data Collection] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Phase 1 involves creating an implementation plan, with definitions including:

- Audience for the plan
- Measurement roles and responsibilities
- Process of measures collection, analysis and reporting
- Details of coordination within the office of the CIO
- Details of coordination between the CISO and other functions within the agency to ensure measures data collection is streamlined and non-intrusive.
- Creation or selection of data collection and tracking tools
- Modification of data collection and tracking tools
- Measures summary reporting formats
- Provisions for continuous monitoring

Any additional input on this section is welcome.

4.2. Collect Data and Analyze Results

This section only has minor updates from [6.2 Collect Data and Analyze Results] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Phase 2 involves activities essential for ensuring that the collected measures are used to gain understanding of information security and identify appropriate actions. These activities include:

- Collect measures data according to the processes in the Measurement Program Implementation Plan
- Aggregate measures as appropriate to derive higher-level measures
- Consolidate collected data and store in a format conducive to data analysis and reporting
- Conduct gap analysis to compare measurements with targets and identify gaps between actual and desired performance
- Identify causes of poor performance
- Identify areas that require improvement

Any additional input on this section is welcome.

4.2.1. Data Collection and Reporting

This section is a new addition to [SP800-55] and will explore how continuous monitoring provides the necessary feedback for calibrating measures and determining the information security program's effectiveness.

Measures data is considered fully automated when all data is gathered by automated data sources without human involvement or intervention. Automation can facilitate continuous monitoring processes of both:

- Measurement data collection
- Measurement data reporting

Detailed information on building a continuous monitoring program can be found in [SP800-137A].

Data may also need to be collected manually in instances where automation of data collection is not a practical option.

- Explores semi-automated and non-automated processes that need humans to facilitate collection or reporting.
- Manual data collection and reporting may also include developing questionnaires, conducting interviews, and administering surveys with the organization's staff.

Any additional input on this section is welcome.

4.3. Identify Corrective Actions

This section only has minor updates from [6.3 Identify Corrective Actions] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Phase 3 consists of developing a plan to serve as the roadmap for closing the implementation gaps identified in Phase 2. This may include:

- Determining the range of corrective actions
- Prioritizing actions based on overall risk mitigation goals
- Selecting the most appropriate corrective actions

Any additional input on this section is welcome.

4.4. Develop a Business Case and Obtain Resources

This section only has minor updates from [6.4 Development Business Case and Obtain Resources] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Phase 4 and 5 addresses the budgeting cycle for acquiring resources needed to implement the corrective actions identified in Phase 3. A business case analysis should feature the results from the previous phases of the information security measurement process. The level of effort for building a business case should correspond with the size and scope of the funding requests. When drafting the business case, it is vital to remember only the organization can establish appetite and tolerance for risk.

Any additional input on this section is welcome.

4.5. Apply Corrective Actions

This section only has minor updates from [6.5 Apply Corrective Actions] in the current [SP800-55] and is intentionally left out of this review cycle.

Summary: Phase 6 involves implementing corrective actions in the information security program or the technical, managerial, or operational areas of security controls. From here the cycle goes back to Phase 2, where data is collected and analyzed. This iterative process allows for the monitoring of progress in the measurement program and ensures corrective actions are influencing information security control implementation in an intended way. Frequent performance measurement will flag actions that are not implemented as planned or not having the desired effects. This enables quick course correction with an organization to avoid problems that could be uncovered in audits, C&A efforts, or to related activities.

References

[CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 6. https://doi.org/10.6028/NIST.CSWP.6

[FIPS200] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200

[IR7358] Bowen P, Kissel RL (2007) Program Review for Information Security Management Assistance (PRISMA). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7358. https://doi.org/10.6028/NIST.IR.7358

[IR8286] Stine KM, Quinn SD, Witte GA, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[MetricsMeasures] Software Quality Group (2021) Metrics and Measures. (National Institute of Standards and Technology, Gaithersburg, MD), https://www.nist.gov/itl/ssd/software-quality-group/metrics-and-measures

[SP800-30] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP800-55] Chew E, Swanson MA, Stine KM, Bartol N, Brown A, Robinson W (2008) Performance Measurement Guide for Information Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-55, Rev. 1. https://doi.org/10.6028/NIST.SP.800-55r1

[SP800-84] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84. https://doi.org/10.6028/NIST.SP.800-84

[SP800-137A] Dempsey KL, PIllitteri VY, Baer C, Niemeyer R, Rudman R, Urban S (2020) Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137A. https://doi.org/10.6028/NIST.SP.800-137A

[SP800-161] Boyens JM, Smith AM, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161r1. https://doi.org/10.6028/NIST.SP.800-161r1

Appendix A. List of Symbols, Abbreviations, and Acronyms

The next draft of this document will include abbreviation and acronym definitions.

Appendix B. Glossary

The next draft of this document will include a Glossary.

Appendix C. Change Log

The final publication of this document will include a summary of changes between Revision 1 and Revision 2.