1 **NIST Special Publication**
2 **NIST SP 800-55r2 iwd**

3 # Performance Measurement Guide
4 # for Information Security

5 Initial Working Draft

6 Katherine Schroeder
7 Hung Trinh

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

10 **NIST Special Publication**
11 **NIST SP 800-55r2 iwd**

12 # Performance Measurement Guide
13 # for Information Security

14 Initial Working Draft

15 Katherine Schroeder
16 Hung Trinh
17 *Computer Security Division*
18 *Information Technology Laboratory*
19
20

23 December 2022

24

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

36 **Disclaimer**

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

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

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

50 **Authority**
51 This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal
52 Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283.
53 NIST is responsible for developing information security standards and guidelines, including minimum requirements
54 for federal information systems, but such standards and guidelines shall not apply to national security systems
55 without the express approval of appropriate federal officials exercising policy authority over such systems. This
56 guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.
57
58 Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding
59 on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be
60 interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or
61 any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and
62 is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

63 **NIST Technical Series Policies**
64 Copyright, Fair Use, and Licensing Statements
65 NIST Technical Series Publication Identifier Syntax

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

69 **How to Cite this NIST Technical Series Publication:**

73 **Author ORCID iDs**

74 Author 1: 0000-0000-0000-0000 [will be added upon final publication]
75 Author 2: 0000-0000-0000-0000

76 **Public Comment Period**

78 **Submit Comments**

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

85 **Abstract**

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

94 **Keywords**

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

96 **Reports on Computer Systems Technology**

107 **Note to Reviewers**

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

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

114   2) How to best communicate information security measurement needs up and down the
115   organizational structure?

116   3) Examples: What kinds of measures and metrics examples or templates could this
117   publication provide that would be helpful in your work?

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

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

123   A [virtual public forum](#) will be held on December 13, 2022, to introduce the working draft of SP
124   800-55 and highlight the various questions for reviewers within the document through a panel of
125   practitioners across different sectors.

126

127

128 **Call for Patent Claims**

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

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

    a) assurance in the form of a general disclaimer to the effect that such party does not hold
137
138   and does not currently intend holding any essential patent claim(s); or

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

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

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

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

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

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

155

Table of Contents

206

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?

207

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.

224 **1.3.   Relation to Other NIST Publications**

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

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

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

239 Any additional input on this section is welcome.

240 **1.4.   Document Organization**

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

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

245 • Chapter 2, Information Security Measures and Fundamentals
246 • Chapter 3, Measurement Program Development Process
247 • Chapter 4, Information Security Measurement Program Implementation

248 Any additional input on this section is welcome.

249 **2. Information Security Measures Fundamentals**

250 **2.1.   Document Conventions**

251 **2.1.1. Terminology**

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

254   • Information security: The protection of information and systems from unauthorized
255   access, use, disclosure, disruption, modification, or destruction to provide confidentiality,
256   integrity, and availability. [FIPS200]
257   • Measurement: The process of experimentally obtaining one or more quantity values that
258   can be reasonably attributed to a quantity. [MetricsMeasures]
259   • Measures: An objective and concrete attribute. Should be quantifiable and observable.
260   Used as the basis for metrics. [MetricsMeasures]
261   • Metrics: Tools designed to facilitate decision-making and improve performance and
262   accountability through collecting, analyzing, and reporting relevant performance-related
263   data. More abstract, higher-level, or subjective than measures. [MetricsMeasures]
264   • Quantitative Assessment: Use a set of methods, principles, or rules for assessing risks
265   based on the use of numbers where the meanings and proportionality of values are
266   maintained inside and outside the context of the assessment. [SP800-30]
267   • Qualitative: Use of a set of methods, principles, or rules for assessing risk based on
268   nonnumerical categories or levels. [SP800-30]
269   • Semi-Quantitative: Use of a set of methods, principles, or rules for assessing risk based
270   on bins, scales, or representative numbers whose values and meanings are not maintained
271   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.*

272

273   Any additional input on this section is welcome.

2.1.2. Definition

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

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

282   • Possible to obtain at different levels within an organization

283   • Based on information security performance goals and objectives

284   • Information security measures monitor the accomplishment of goals and objectives by
285   quantifying the implementation, efficiency, and effectiveness of security controls.

286   • Data required for calculating measures must be readily obtainable, and the process under
287   consideration needs to be measurable.

288   • Allow for tracking performance and directing resources.

289   Any additional input on this section is welcome.

2.2.   Benefits of Using Measures

291
292
293

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.

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

296   •   Increase Accountability
297   •   Improve Information Security Effectiveness
298   •   Demonstrate Compliance
299   •   Provide Quantifiable Inputs for Resource Allocation Decisions

300   New Additions:

301   •   Manage Risk
302   •   Continuous Analysis

303   Any additional input on this section is welcome.

2.3.   Critical Success Factors

305
306
307

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.

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

310   •   Foundation of strong upper-level management support
311   •   Practical information security policies & procedures
312   •   Quantifiable performance measures
313   •   Results-oriented measures and analysis
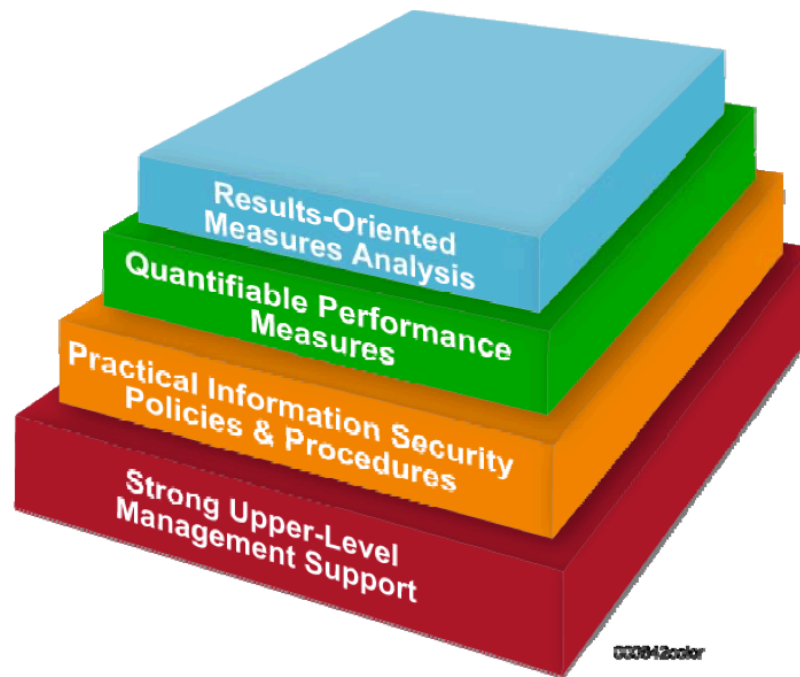
314

315 **Fig. 1.** Information Security Measurement Program Structure

316 Any additional input on this section is welcome.

317 2.4. Types of Measures

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

320 Summary: Organizational maturity determines the types of measures an organization can gather
321 successfully. The existence and institutionalization of processes and procedures define this
322 maturity. This section explores types of measures – implementation, effectiveness/efficiency,
323 and business impact – against the measurement of processes, operating procedures, data
324 availability, collection difficulty, collection automation.
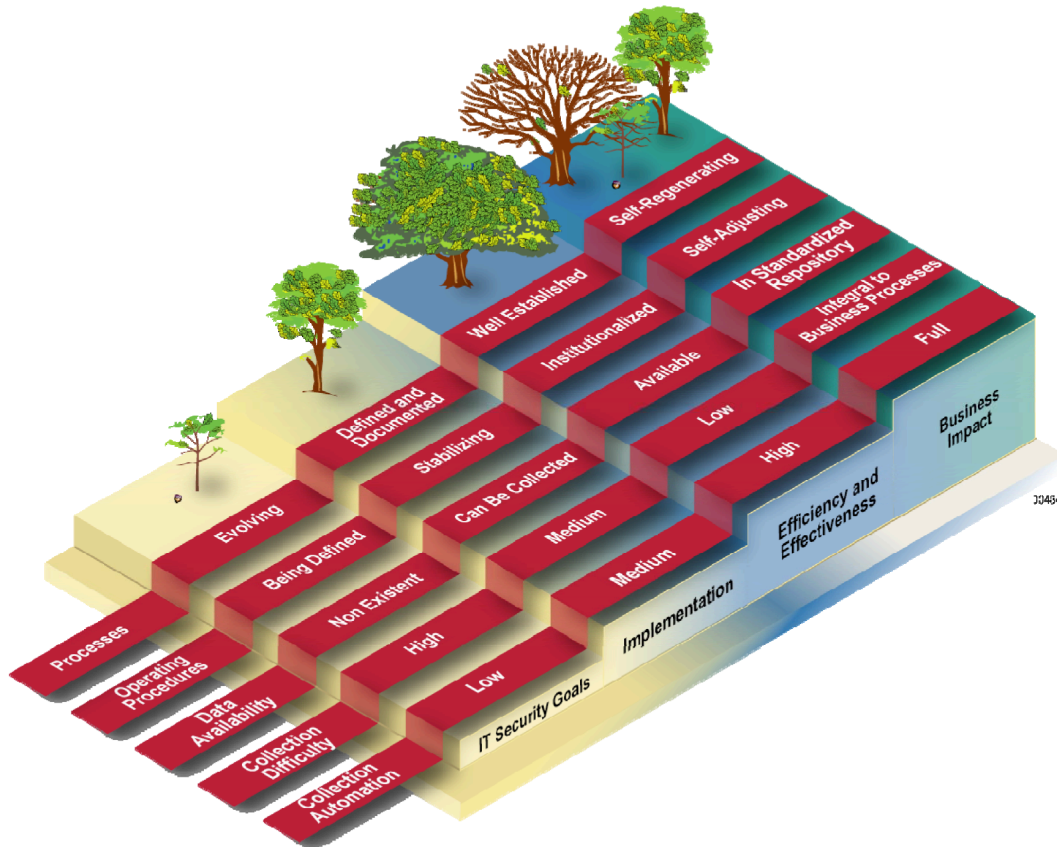
325

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

327   Any additional input on this section is welcome.

328   **2.4.1. Implementation Measures**

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

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

336   Any additional input on this section is welcome.

337 ### 2.4.2. Effectiveness/Efficiency Measures

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

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

349 Any additional input on this section is welcome.

350 ### 2.4.3. Impact Measures

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

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

358 Any additional input on this section is welcome.

359 ## 2.5. Measurement Considerations

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

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

367 Any additional input on this section is welcome.

368   ### 2.5.1. Organizational Considerations

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

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

377   Any additional input on this section is welcome.

378   ### 2.5.2. Manageability

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

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

387   Any additional input on this section is welcome.

388   ### 2.5.3. Data Management Concerns

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

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

398   Any additional input on this section is welcome.

399 ### 2.5.4. Measurement Quality

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

402 • Clearly defined data gathering and reporting requirements
403 • Standardizing the measurement process
404 • Data quality and validity
405 • Tracking changes over time to ensure consistency
406 • Repeatability of processes

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

407

408 Any additional input on this section is welcome.

409 ### 2.5.5. Trends and Historical Information

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

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

419 Any additional input on this section is welcome.

420 ### 2.5.6. Automation of Data Collection

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

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

429   Any additional input on this section is welcome.

2.6.   Information Security Measurement Program Scope

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

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

441   Any additional input on this section is welcome.

2.6.1. System Level

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

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

2.6.2. Enterprise-wide Program

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

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

460   Any additional input on this section is welcome.

461 3. Measures Development Process

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

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

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

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

473 1. Stakeholders and interests
474 2. Goals and objectives
475 3. Information security policies, guidelines, and procedures
476 4. Information security program implementation
477 5. Level of implementation
478 6. Program results
479 7. Business/mission impact
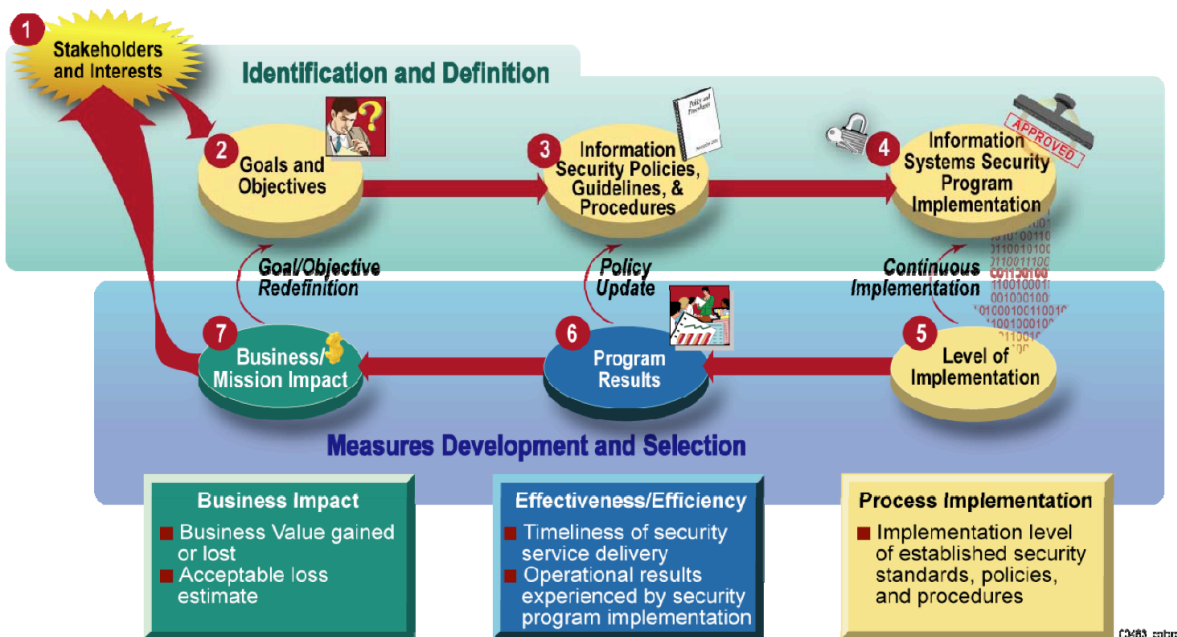
480

481 **Fig. 3.** Information Security Measurement Development Process

482   Any additional input on this section is welcome.

3.1.   Stakeholder Identification

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

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

490   Any additional input on this section is welcome.

3.2.   Goals and Objective Definition

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

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

499   Any additional input on this section is welcome.

3.2.1. Governance and Compliance

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

504   • Governance structures
505   • Laws and regulations
506   • Industry guidance
507   • Various requirements from outside the organizational structure, such as:
508   o Insurance
509   o Auditors
510   o Accreditation bodies
511   o 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.

512

513 Any additional input on this section is welcome.

3.3. Information Security Policies, Guidelines, and Procedures Review

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

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

521 Any additional input on this section is welcome.

3.4. Information Security Measurement Program Implementation Review

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

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

529 Any additional input on this section is welcome.

3.5. Measures Development and Selection

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

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

536 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   o Copula methods for correlation between risks
575   o Event Tree analysis
576   o Machine learning and predictive models
577   • Consequences
578   o Establish a consequence model by looking at potential events and their outcomes.
579   o 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   o Expected shortfall
583   o Value at risk – statistical analysis of historical market trends
584   o 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.

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.

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

606 - Success hitting control targets
607 - Indicators
608   o Key performance indicators
609   o Key goal indicators
610   o Key risk indicators
611   o Critical success factors
612   o Leading and lagging indicators
613 - False positive report rate
614 - Incident response volume
615 - Frameworks
616 - Maturity modeling
617 - Compliance
618 - Audits
619 - Penetration testing
620 - Bug bounties

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

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

623

624 Any additional input on this section is welcome.

3.7. Measures Development Template

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

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

634   o Measure ID
635   o Goal
636   o Measure
637   o Type
638   o Formula
639   o Target

640   o   Implementation evidence
641   o   Frequency
642   o   Responsible parties
643   o   Data source
644   o   Reporting format

645   Any additional input on this section is welcome.

3.8. Feedback Within the Development Process

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

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

651   o   Measuring performance
652   o   Identifying causes of unsatisfactory performance
653   o   Pinpointing improvement areas
654   o   Facilitating consistent policy implementation
655   o   Effecting security policy changes
656   o   Redefining goals and objectives
657   o   Supporting continuous improvement

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

660   Any additional input on this section is welcome.

4. Information Security Measurement Program Implementation

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

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

670

Fig. 4. Information Security Measurement Program Implementation Process

672   Any additional input on this section is welcome.

4.1.   Prepare for Data Collection

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

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

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

688   Any additional input on this section is welcome.

4.2.   Collect Data and Analyze Results

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

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

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

704   Any additional input on this section is welcome.

4.2.1. Data Collection and Reporting

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

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

713   o   Measurement data collection
714   o   Measurement data reporting

715   Detailed information on building a continuous monitoring program can be found in [SP800-
716   137A].

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

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

723   Any additional input on this section is welcome.

4.3.   Identify Corrective Actions

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

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

730   o Determining the range of corrective actions
731   o Prioritizing actions based on overall risk mitigation goals
732   o Selecting the most appropriate corrective actions

733 Any additional input on this section is welcome.

4.4. Develop a Business Case and Obtain Resources

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

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

744 Any additional input on this section is welcome.

4.5. Apply Corrective Actions

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

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

References

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

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

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

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

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

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

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

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

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

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

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

799   **Appendix A. List of Symbols, Abbreviations, and Acronyms**

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

801   **Appendix B. Glossary**

802   The next draft of this document will include a Glossary.

803   **Appendix C. Change Log**

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

806