



**NIST Special Publication 800**  
**NIST SP 800-55v2 ipd**

# **Measurement Guide for Information Security**

*Volume 2 — Developing an Information Security  
Measurement Program*

Initial Public Draft

Katherine Schroeder  
Hung Trinh  
Victoria Yan Pillitteri

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-55v2.ipd>

**NIST Special Publication 800**  
**NIST SP 800-55v2 ipd**

# **Measurement Guide for Information Security**

*Volume 2 — Developing an Information Security  
Measurement Program*

Initial Public Draft

Katherine Schroeder  
Hung Trinh  
Victoria Yan Pillitteri  
*Computer Security Division  
Information Technology Laboratory*

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-55v2.ipd>

January 2024



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*

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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, 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 included in final publication]

Supersedes NIST Series XXX (Month Year) DOI

### **How to Cite this NIST Technical Series Publication**

Schroeder K, Trinh H, Pillitteri V (2024) Measurement Guide for Information Security: Volume 2 — Developing an Information Security Measurement Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-55v2 ipd. <https://doi.org/10.6028/NIST.SP.800-55v2.ipd>

### **Author ORCID iDs**

Katherine Schroeder: 0000-0002-4129-9243

Hung Trinh: 0000-0002-3323-0836

Victoria Yan Pillitteri: 0000-0002-7446-7506

NIST SP 800-55v2 ipd (Initial Public Draft)  
January 2024

Measurement Guide for Information Security  
Volume 2 — Developing a Measurement Program

**Public Comment Period**

January 17, 2024 – March 18, 2024

**Submit Comments**

[cyber-measures@list.nist.gov](mailto: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).**

1 **Abstract**

2 This document provides guidance on how an organization can develop an information security  
3 measurement program with a flexible structure for approaching activities around the  
4 development and implementation of information security measures.

5 **Keywords**

6 assessment; information security; measurement; measures; metrics; performance; program;  
7 reports; security controls.

8 **Reports on Computer Systems Technology**

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

19 **Audience**

20 This guide is written primarily for users with responsibilities or interest in information security  
21 measurement and assessment. Government and industry can use the concepts, processes, and  
22 candidate measures presented in this guide.

23

24 **Call for Patent Claims**

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

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

- 34 a) assurance in the form of a general disclaimer to the effect that such party does not hold  
35 and does not currently intend holding any essential patent claim(s); or
- 36 b) assurance that a license to such essential patent claim(s) will be made available to  
37 applicants desiring to utilize the license for the purpose of complying with the guidance  
38 or requirements in this ITL draft publication either:
- 39 i. under reasonable terms and conditions that are demonstrably free of any unfair  
40 discrimination; or
- 41 ii. without compensation and under reasonable terms and conditions that are  
42 demonstrably free of any unfair discrimination.

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

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

50 Such statements should be addressed to: [cyber-measures@list.nist.gov](mailto:cyber-measures@list.nist.gov)

51

52 **Note to Reviewers**

53 The initial public drafts (ipd) of NIST Special Publication (SP) 800-55, *Measurement Guide for*  
54 *Information Security, Volume 1 – Identifying and Selecting Measures* and *Volume 2 – Developing*  
55 *an Information Security Measurement Program* are available for comment after extensive  
56 research, development, and customer engagement.

57 In response to the feedback from the pre-draft call for comment and initial working draft  
58 (annotated outline), NIST continued to refine the publications by organizing the guidance into  
59 two volumes and developing more actionable and focused guidance in each.

- 60 • *Volume 1 – Identifying and Selecting Measures* – is a flexible approach to the  
61 development, selection, and prioritization of information security measures. This  
62 volume explores both quantitative and qualitative assessment and provides basic  
63 guidance on data analysis techniques as well as impact and likelihood modeling.
- 64 • *Volume 2 – Developing an Information Security Measurement Program* - is a  
65 methodology for developing and implementing a structure for an information security  
66 measurement program.

67 Reviewers are encouraged to comment on all or parts of draft NIST SP 800-55 *Measurement*  
68 *Guide for Information Security, Volume 1 – Identifying and Selecting Measures*, and *Volume 2*  
69 *– Developing an Information Security Measurement Program*. NIST request comments be  
70 submitted to [cyber-measures@list.nist.gov](mailto:cyber-measures@list.nist.gov) by 11:59 PM Eastern Time (ET) on March 18, 2024.  
71 Commenters are encouraged to use the comment template provided with the document  
72 announcement.

73

74	<b>Table of Contents</b>	
75	<b>1. Introduction</b> .....	<b>1</b>
76	1.1. Purpose and Scope.....	1
77	1.2. Relationship to Other Publications .....	1
78	1.3. Document Organization .....	2
79	1.4. Document Terminology .....	2
80	<b>2. Fundamentals</b> .....	<b>3</b>
81	2.1. Measurement Program Benefits.....	3
82	2.2. Program Scope .....	3
83	2.3. Foundations for a Successful Information Security Measurement Program.....	4
84	2.4. Roles and Responsibilities .....	5
85	2.5. Programmatic Value of Metrics .....	8
86	2.6. Aggregation and Communication .....	8
87	2.7. Measurement Program Considerations.....	9
88	2.7.1. Organizational Considerations .....	9
89	2.7.2. Manageability .....	10
90	2.7.3. Data Management Concerns.....	10
91	<b>3. Information Security Measurement Program</b> .....	<b>11</b>
92	3.1. Evaluation and Definition of the Existing Security Program .....	12
93	3.1.1. Gathering Stakeholder Input .....	13
94	3.1.2. Goals and Objectives .....	13
95	3.1.3. Information Security Policies, Procedures, and Guidelines .....	13
96	3.1.4. Evaluating Current Implementation.....	14
97	3.2. Identify and Prioritize Measures.....	14
98	3.3. Identify and Prioritize Measures.....	18
99	3.3.1. Identify and Prioritize Measures .....	19
100	3.3.2. Identify Corrective Actions.....	20
101	3.3.3. Apply Corrective Actions .....	21
102	<b>References</b> .....	<b>22</b>
103	<b>Appendix A. Glossary</b> .....	<b>23</b>
104	<b>Appendix B. Change Log</b> .....	<b>24</b>
105	<b>List of Figures</b>	
106	<b>Fig. 1. Information security measurement program structure</b> .....	<b>4</b>
107	<b>Fig. 2. Information security measurement program workflow</b> .....	<b>11</b>

108	<b>Fig. 3. Evaluation and definition of the existing security program .....</b>	<b>12</b>
109	<b>Fig. 4. Identify and prioritize measures .....</b>	<b>15</b>
110	<b>Fig. 5. Information security program development and types of measurement.....</b>	<b>17</b>
111	<b>Fig. 6. Information security measures development process.....</b>	<b>18</b>
112	<b>Fig. 7. Information security measurement implementation .....</b>	<b>19</b>
113		

## 114 **1. Introduction**

115 Organizational, financial, and regulatory reasons drive the desire to build a robust information  
116 security measurement program. Such programs facilitate decision-making and improve  
117 performance and accountability by providing a structure for collecting, analyzing, and reporting  
118 relevant and related data. Organizations can use measures as management tools in their  
119 internal improvement efforts and link the implementation of their information security  
120 programs to agency- and enterprise-level planning efforts.

### 121 **1.1. Purpose and Scope**

122 NIST Special Publication (SP) 800-55v2 (Volume 2) is a guide for developing and implementing  
123 an information security measurement program. The term “program” in SP 800-55v2 is intended  
124 to signify a flexible structure for approaching activities around the development and  
125 implementation of information security measures. While “program” is used in the development  
126 and implementation of cybersecurity measures, a measurement program can be part of an  
127 existing cybersecurity program or its own dedicated effort. Measures provide the means for  
128 tying information security policy, procedure, and control implementation, efficiency, and  
129 effectiveness to an organization’s success in its business activities. In this document, the term  
130 “controls” is used broadly to describe identified countermeasures to manage information  
131 security risks. It is intended to be framework- or standard-agnostic and can also apply to other  
132 existing models or frameworks that might be used in an organization.

133 Where this document provides a methodology for developing and implementing an information  
134 security measurement program, SP 800-55v1 addresses the selection and development of  
135 information security measures. SP 800-55v2 discusses the concept of organizational or program  
136 maturity but is not intended for use as a maturity model and is intentionally agnostic toward  
137 any specific maturity models.

### 138 **1.2. Relationship to Other Publications**

139 This document is intended to provide considerations for measuring the information security  
140 program activities described in several NIST publications, including:

- 141 • SP 800-137A, *Assessing Information Security Continuous Monitoring Programs*
- 142 • *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST  
143 Cybersecurity Framework) [1]
- 144 • SP 800-30r1 (Revision 1), *Guide for Conducting Risk Assessments* [2]
- 145 • SP 800-37r2, *Risk Management Framework for Information Security Systems and*  
146 *Organizations: A System Life Cycle Approach for Security and Privacy* [3]
- 147 • SP 800-161r1, *Cybersecurity Supply Chain Risk Management Practices for Systems and*  
148 *Organizations* [4]

- 149       • Internal Report (IR) 8286, *Identifying and Estimating Cybersecurity Risk for Enterprise*  
150       *Risk Management (ERM)* [5]

### 151   **1.3. Document Organization**

152   The remaining sections of this document discuss the following:

- 153       • Section 2, Fundamentals
- 154       • Section 3, Information Security Measurement Program
- 155       • Appendix A, Glossary
- 156       • Appendix B, Change Log

### 157   **1.4. Document Terminology**

158   In the context of this document, the follow terms are defined as follows:

- 159       • **Information security:**<sup>1</sup> The protection of information and systems from unauthorized  
160       access, use, disclosure, disruption, modification, or destruction to provide  
161       confidentiality, integrity, and availability. [6]
- 162       • **Assessment:** The action of evaluating, estimating, or judging against defined criteria.  
163       Different types of assessment (i.e., qualitative, quantitative, and semi-quantitative) are  
164       used to assess risk. Some types of assessment yield measures.
- 165       • **Assessment result:** The output or outcome of an assessment.
- 166       • **Qualitative assessment:** The use of a set of methods, principles, or rules for assessing  
167       risk based on non-numerical categories or levels. [2]
- 168       • **Quantitative assessment:** The use of a set of methods, principles, or rules for assessing  
169       risks based on the use of numbers where the meanings and proportionality of values are  
170       maintained inside and outside the context of the assessment. [2]
- 171       • **Semi-quantitative assessment:** The use of a set of methods, principles, or rules for  
172       assessing risk based on bins, scales, or representative numbers whose values and  
173       meanings are not maintained in other contexts. [2]
- 174       • **Measurement:** The process of obtaining quantitative values using quantitative methods.
- 175       • **Measures:** Quantifiable and objective values resulting from measurement.
- 176       • **Metrics:** Measures and assessment results designed to track progress, facilitate  
177       decision-making, and improve performance with respect to a set target.

---

<sup>1</sup> The term “cybersecurity” can be used interchangeably with “information security.”

## 178 **2. Fundamentals**

179 A comprehensive information security measurement program provides substantive  
180 justifications for decisions that directly affect the information security posture of an  
181 organization, including budget and personnel requests and the allocation of available resources.  
182 A measurement program covers an evaluation of the existing security program, the  
183 identification and prioritization of potential measures, and an implementation structure for  
184 collecting data and applying corrective actions based on the findings of those measures. Having  
185 a structure to develop and implement information security measures allows for a repeatable  
186 and archivable process. An information security measurement program also assists in preparing  
187 required reports related to information security performance. For this reason, a measurement  
188 program needs support from across the organizational structure.

### 189 **2.1. Measurement Program Benefits**

190 Organizations want to know how well they are managing their information security risk,  
191 whether their personnel are sufficiently educated and trained to minimize risks to the  
192 organization, and whether a new service or technology might better serve their security  
193 posture. A measurement program can answer questions about information security risk  
194 management by providing a structure that helps organizations collect and analyze data. It can  
195 also enable discussions and communication around measures and the goals of measurement.  
196 Where measures and metrics provide data, the program itself provides a broader context and  
197 lens to consistently interpret, analyze, and communicate the larger impacts of information  
198 security measures.

199 Additionally, an information security measurement program can increase accountability by  
200 helping organizations identify specific controls that are implemented incorrectly, are not  
201 implemented, or are ineffective. The continuous feedback provided by a structured  
202 measurement program supports regular internal communications that collect data about  
203 information security performance and risks for high-level members of the organization.  
204 Implementing an information security measurement program demonstrates organizational  
205 commitment to proactive information security and continuous improvement. When using the  
206 appropriate measures, an information security measurement program enables organizations to  
207 quantify improvements in securing systems and demonstrate quantifiable progress in  
208 accomplishing strategic goals and objectives. More information on selecting measures can be  
209 found in SP 800-55v1.

### 210 **2.2. Program Scope**

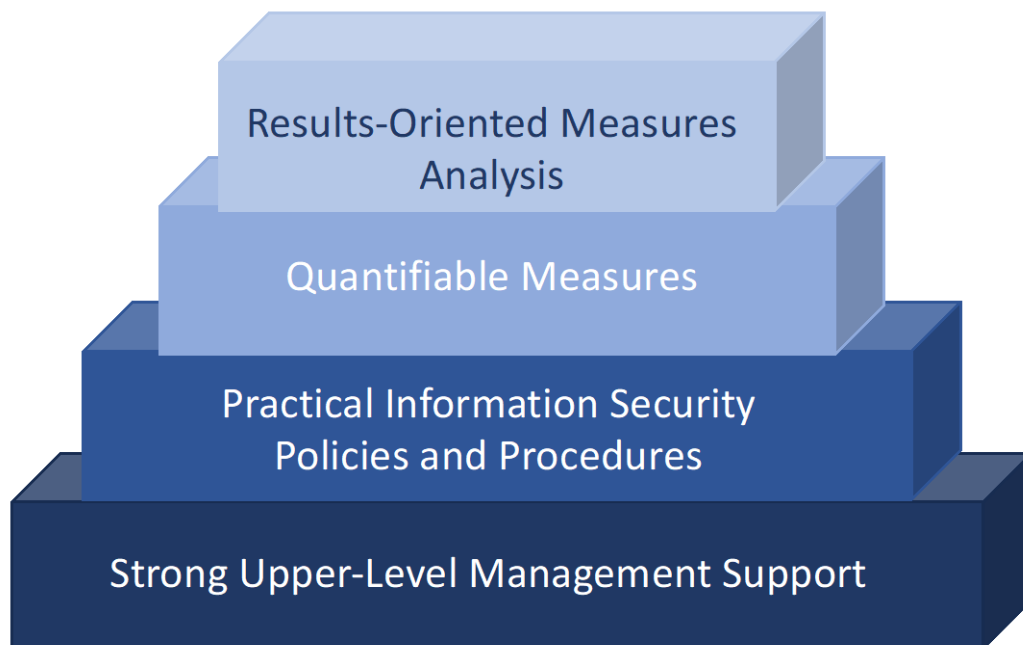
211 To ensure the success of program-level measurement, the organization has consistent,  
212 repeatable processes and data availability across the enterprise. In a successful measurement  
213 program, these processes are customized to the different environments and needs of the  
214 individual organization. Measures can be applied to organizational units, sites, or other  
215 constructs to meet specific stakeholder requirements, strategic goals, operating environments,  
216 risk priorities, and information security program maturity.

217 Information security measurement can be implemented at the individual system level to  
218 provide quantifiable data regarding the implementation, effectiveness, and impact of controls.  
219 This can help system owners determine the security posture of their system, demonstrate  
220 compliance with organizational requirements, and identify areas for improvement. Information  
221 security measurement can also be implemented at a program level to monitor and measure the  
222 implementation, effectiveness, efficiency, and impact of information security activities across  
223 the organization. In short, an information security measurement program provides a  
224 mechanism to aggregate measures and support organization-wide decision-making.

### 225 **2.3. Foundations for a Successful Information Security Measurement Program**

226 An information security measurement program includes four interdependent components, as  
227 shown in **Fig. 1**:

- 228 1. A foundation of strong upper-level management support
- 229 2. Practical information security policies and procedures
- 230 3. Quantifiable measures
- 231 4. Results-oriented measures analysis



232

233 **Fig. 1. Information security measurement program structure**

234 A foundation of strong upper-level management support is critical to the success of an  
235 information security program. This support establishes a focus on information security within

236 the highest levels of the organization. The information security measurement program can fail  
237 under the pressure of organizational dynamics and budget limitations without the proactive  
238 support of personnel in positions that control information resources.

239 An effective information security measurement program also has information security policies  
240 and procedures backed by the authority necessary to enforce compliance and manage risk.  
241 Information security policies define the information security management structure, assign  
242 information security responsibilities, and create the foundation needed to reliably measure  
243 progress. The related procedures document management’s position on implementing  
244 information security controls and the rigor with which they are applied. Measures are not easily  
245 obtainable if there are no procedures to supply data for measurement.

246 Quantifiable measures based on performance objectives are be developed and established to  
247 capture and provide meaningful performance data. The goal of these measure is to be easily  
248 obtainable, feasible to measure, and repeatable, in order to show relevant performance trends,  
249 track performance, and direct resources.

250 Finally, the information security measurement program will emphasize consistent periodic  
251 analyses of the measures data. Lessons learned from these analyses can improve the  
252 effectiveness of existing controls and help plan the implementation of future controls. To  
253 ensure that the collected data is meaningful and useful, stakeholders and users will prioritize  
254 accurate data collection. More information on quantifiable measures and measures analysis  
255 can be found in SP 800-55v1.

## 256 **2.4. Roles and Responsibilities**

257 This section outlines the key roles and responsibilities for developing and implementing an  
258 information security measurement program. While information security is the responsibility of  
259 all organization members, the positions described here are specific to key information security  
260 stakeholders. Organizations have varying missions, business functions, and organizational  
261 structures, so there may be differences in naming conventions and how responsibilities are  
262 allocated across organizational personnel. The functions and responsibilities listed below will be  
263 owned by someone within the organizational structure even when organizational structures  
264 vary. The application of a measurement program as described in this publication is intended to  
265 be flexible and allow organizations to manage their measurement needs.

### 266 **Chief Executive Officer/Agency Head**

267 The information security measurement responsibilities of the Chief Executive Officer (CEO) or  
268 agency head include:

- 269 • Ensuring that information security measures are used in support of strategic and  
270 operational planning processes to secure the organization’s mission
- 271 • Ensuring that the Chief Information Officer (CIO) or Chief Information Security Officer  
272 (CISO) integrates information security measures into annual reporting on the  
273 effectiveness of the information security program

- 274 • Demonstrating support for information security measures development and  
275 implementation and communicating official support to the organization
- 276 • Ensuring that information security measurement activities have adequate financial and  
277 human resources for success
- 278 • Actively promoting information security measurement as an essential facilitator of  
279 information security performance improvement throughout the organization
- 280 • Approving policies to officially institute measures collection

## 281 **Chief Information Officer<sup>2</sup>**

282 The information security measurement responsibilities of the Chief Information Officer (CIO)  
283 include:

- 284 • Ensuring the development and implementation of an information security measurement  
285 program
- 286 • Using information security measures to assist in monitoring compliance with applicable  
287 information security requirements
- 288 • Using information security measures to report on the effectiveness of the organization's  
289 information security program
- 290 • Demonstrating management's commitment to the development and implementation of  
291 information security measures through formal leadership
- 292 • Formally communicating the importance of using information security measures to  
293 monitor the overall health of the information security program and comply with  
294 applicable regulations
- 295 • Allocating adequate financial and human resources to the information security  
296 measurement program
- 297 • Regularly reviewing information security measures and using that data to support  
298 policies, resource allocation, budget decisions, and assessments of the information  
299 security program's posture and operational risks to agency information systems
- 300 • Ensuring that a process is in place to address issues discovered through measures  
301 analysis and taking corrective actions, such as revising information security procedures  
302 and providing additional information security training to staff
- 303 • Issuing policies, procedures, and guidelines to officially develop, implement, and  
304 institute measures

---

<sup>2</sup> When a federal agency has not designated a formal CIO position, FISMA requires the associated responsibilities to be handled by a comparable agency official.

305 **Chief Information Security Officer**

306 The information security measurement responsibilities of the Chief Information Security Officer  
307 (CISO) include:

- 308 • Developing and implementing information security measures
- 309 • Integrating information security measurement into the process for planning,  
310 implementing, evaluating, and documenting remedial actions to address any  
311 deficiencies in the organization’s information security policies, procedures, and  
312 practices
- 313 • Obtaining adequate financial and human resources to support the development and  
314 implementation of an information security measurement program
- 315 • Leading the development of any internal guidelines or policies related to information  
316 security measures
- 317 • Using information security measures to report on the effectiveness of the organization’s  
318 information security program, including remedial actions
- 319 • Ensuring that a standard process is used throughout the organization for information  
320 security measures development, creation, analysis, and reporting
- 321 • Using information security measures for policy, resource allocation, and budget  
322 decisions

323 **Program Managers and System Owners**

324 The information security measurement responsibilities of program managers and system  
325 owners include:

- 326 • Participating in information security measurement program development and  
327 implementation by providing feedback on the feasibility of data collection and  
328 identifying data sources and repositories
- 329 • Educating staff on the development, collection, analysis, and reporting of information  
330 security measures and their effects on information security policy, requirements,  
331 resource allocation, and budget decisions
- 332 • Ensuring that measurement data is consistently and accurately collected and provided  
333 to designated staff for analysis and reporting
- 334 • Directing the full participation and cooperation of staff, when required
- 335 • Regularly reviewing information security measures data and using it for policy, resource  
336 allocation, and budget decisions
- 337 • Supporting the implementation of corrective actions identified through measuring  
338 information security performance

### 339 **Other Roles**

340 The information security measurement responsibilities of those who report to program  
341 managers or system owners include:

- 342 • Participating in the development and implementation of an information security  
343 measurement program by providing feedback on the feasibility of data collection and  
344 identifying data sources and repositories
- 345 • Collecting data or providing measurement data to designated staff who are collecting,  
346 analyzing, and reporting data

347 Information security measurement may require inputs from various organizational components  
348 or stakeholders, including incident response, information technology operations, privacy,  
349 enterprise architecture, human resources, physical security, and others.

### 350 **2.5. Programmatic Value of Metrics**

351 Metrics are designed to track progress, facilitate decision-making, and improve performance by  
352 providing insight into how an organization is performing. Metrics may be the results of  
353 measurements or assessments of trends, and they provide a common language for technical  
354 teams and management to discuss information security. Metrics can also help prioritize areas  
355 for growth, improvement, or the reallocation of resources.

356 By keeping metrics consistent over time, a measurement program can evaluate long-term  
357 trends and expected ranges. A new metric may provide important insights, but tracking the  
358 measurements related to metrics over a continuous period (e.g., quarter to quarter, year to  
359 year) will give more information about the success of organization-, program-, and system-level  
360 information security plans, policies, procedures, and goals. Metrics enable goal setting against  
361 industry standards and internal targets. An organization may find a wide variety of metrics to fit  
362 their needs, and by utilizing the findings of an information security measurement program, the  
363 organization will be better prepared to make decisions about measures and track changes.

### 364 **2.6. Aggregation and Communication**

365 An information security measurement program plays a crucial role in enhancing organizational  
366 communication and providing insights to higher-level management and executives.  
367 Measurements provide quantifiable data about an organization's information security posture,  
368 such as incident response time. This data can then be used to make informed decisions about  
369 resource allocation, risk mitigation strategies, and investment priorities.

370 Data from various sources like vulnerability scans, incident logs, and compliance assessments  
371 can be aggregated to give executives a larger picture of information security. Summarizing  
372 measurement findings and metrics into concise reports facilitates efficient communication.  
373 Regularly reporting on measurement and assessment results fosters transparency by providing  
374 visibility into security operations, promotes accountability for meeting performance targets,

375 and encourages continuous improvements. When findings are shared with executives, they  
376 demonstrate the organization's commitment to its information security posture.

377 While incredibly valuable, a common challenge is determining what data to include and how to  
378 aggregate large amounts of data to tell a meaningful story. When communicating about  
379 information security measurement, an organization will consider the goals of the reporting. For  
380 example, when aggregating measures to communicate about risk the following considerations  
381 are helpful:

- 382 • What measures tell a more precise risk story?
- 383 • What measures will be best understood by the recipient?
- 384 • What measures deliver risk insights most effectively?

385 Organizations may want to combine the results of individual measures or metrics to show  
386 aggregated data. Gaining insight requires measures that have meaning and context within the  
387 organization. Ultimately, the needs of an individual organization will determine what data to  
388 aggregate and report on in communications. More information on developing, selecting, and  
389 evaluating measures that fit the needs of an organization can be found in SP 800-55v1.

390 Aggregation and communication about information security measures can be small or large and  
391 casual or formal. For example, short memos may respond to direct questions and only show  
392 one or two measures, whereas a formal annual report may include more detailed information  
393 about the organization's information security posture, risks, audits, confirmed findings, and  
394 compliance. A larger annual report will require measures related to all the topics covered in the  
395 report. The specific needs and reporting structure of a request for information will determine  
396 what data needs to be aggregated.

397 Programs that ensure consistent and reliable information security measurement empower  
398 organizations to communicate effectively, make informed decisions, and align security efforts  
399 with business objectives. As the information security program evolves, standardized  
400 measurement practices will further enhance communication across all levels of the  
401 organization.

## 402 **2.7. Measurement Program Considerations**

403 When an organization is building a measurement program, it will consider the specific  
404 organizational structure, processes, required budget, personnel, and time resources to make  
405 the program successful.

### 406 **2.7.1. Organizational Considerations**

407 The development and implementation of information security measures will be coordinated  
408 with appropriate stakeholders from relevant organizational elements. Include those who  
409 regularly interact with information security even if it is not their primary responsibility, such as  
410 the training, resource management, and legal departments. The program will also comply with  
411 any existing processes for approving organization-wide data calls and actions. Effective

412 coordination among different organizational elements can ensure that information security  
413 measures are implemented uniformly across the organization.

#### 414 **2.7.2. Manageability**

415 Organizations need to be able to manage their information security measurement program.  
416 Here, “manageability” refers to having the organizational resources to support the  
417 measurement program’s goals and objectives. The results of many information security  
418 activities can be quantified and used for measurement. However, since resources are limited,  
419 organizations prioritize measurement requirements to ensure that a limited number of  
420 measures are gathered. Ensuring that each stakeholder is responsible for as few measures as  
421 possible may make the collected measures are meaningful, yield impact and outcome findings,  
422 and provide stakeholders with the time necessary to address performance gaps. As the  
423 program continues to develop and target levels of measurement are reached, obsolete  
424 measures are phased out, and new measures that show the completion and effectiveness of  
425 more current items are used.<sup>3</sup> Further measures will also be required if the organization’s  
426 mission is redefined or if changes are made to information security policies and guidelines.

#### 427 **2.7.3. Data Management Concerns**

428 Having an information security measurement program in place helps organizations establish  
429 consistent and well-defined methods for collecting security-related data, including defining  
430 what data to collect, how to collect it, and at what intervals. Operationally, this may include  
431 identifying relevant data sources, determining granularity, and validating data accuracy. The  
432 information security measurement program also can ensure that clear metadata is used by  
433 defining how data will be normalized with consistent units and formats and ensuring accurate  
434 aggregation and meaningful comparisons. As effective reporting processes are aligned with the  
435 information security measurement program’s goals, taking the time to establish a consistent  
436 data management environment provides a solid foundation for gathering and aggregating  
437 measures data.

438

---

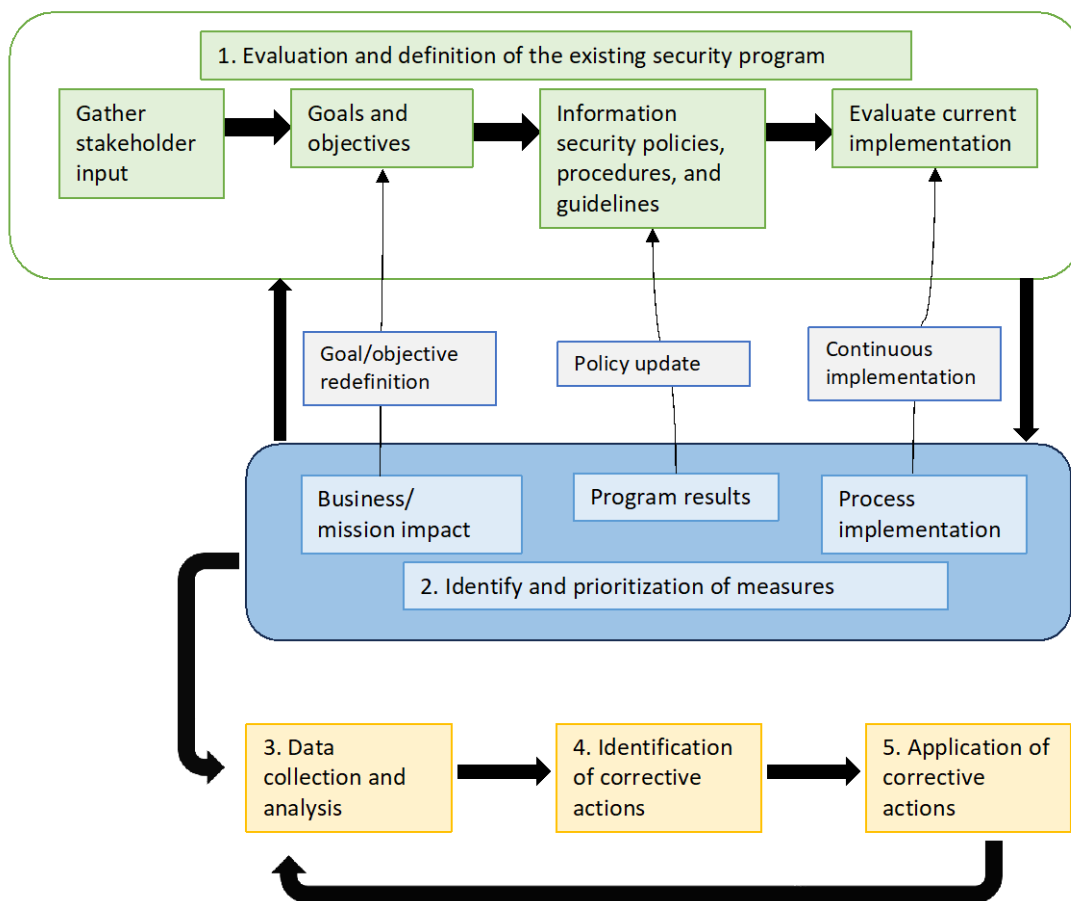
<sup>3</sup> Section 3.2 discusses the use of organizational maturity and the progress of the measurement program as a basis for what types of measurement can be collected.

### 439 3. Information Security Measurement Program

440 The workflow of implementing an information security measurement program consists of five  
441 major activities:

- 442 1. Evaluation and definition of the existing security program
- 443 2. Identification and prioritization of measures
- 444 3. Data collection and analysis
- 445 4. Identification of corrective actions
- 446 5. Application of corrective actions

447 The activities outlined in **Fig. 2** do not need to be done sequentially. The process is provided in a  
448 linear form to encourage the use of a consistent yet flexible methodology that can be tailored  
449 to a specific organization and its unique stakeholder groups to develop and implement an  
450 information security measurement program. The process can be applied across different levels  
451 of the organization.



452

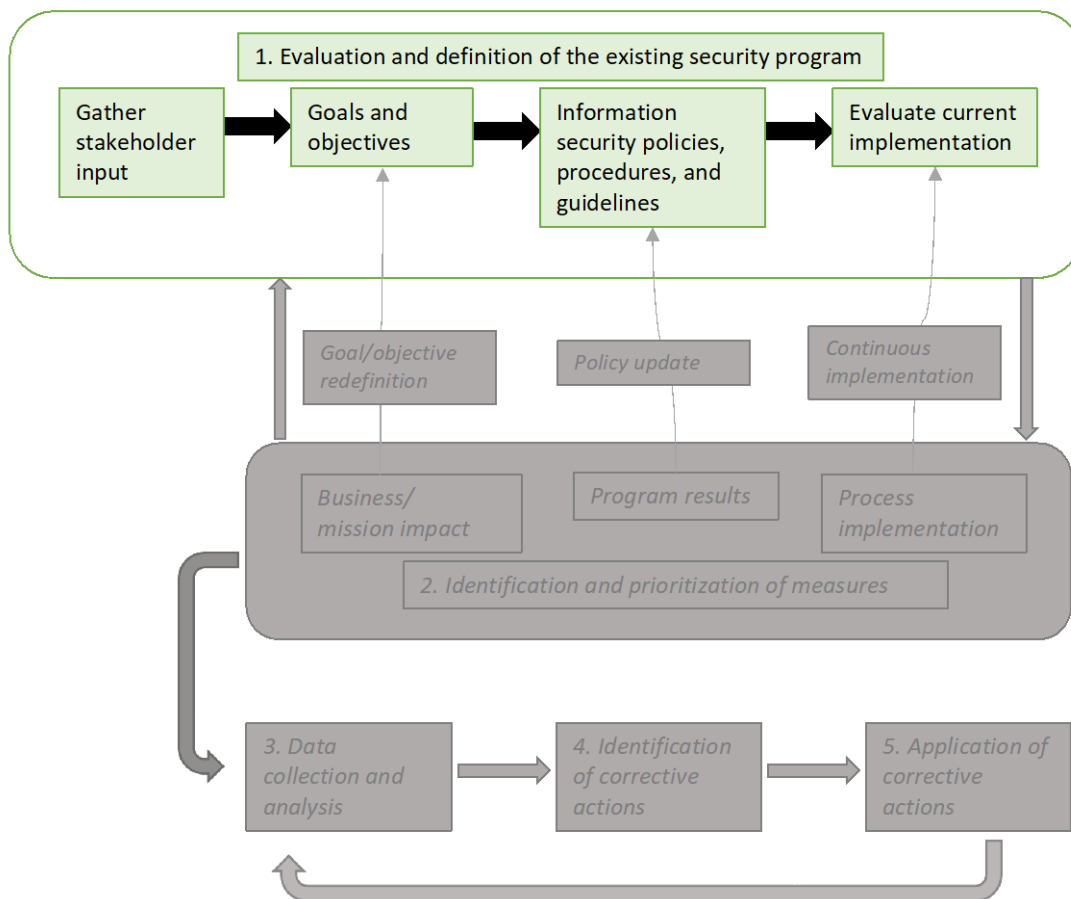
453

Fig. 2. Information security measurement program workflow

### 3.1. Evaluation and Definition of the Existing Security Program

Organizations will first identify their measurement needs when building and maintaining an information security measurement program. This initial effort is more effective than retrofitting measures, though measures may need to be changed in the future. Ultimately, there is value in having both stability and flexibility in the organizational measures that are selected. Important considerations for establishing an information security measurement program include:

- Selecting the measures that are most appropriate for the organization’s strategy and business environment, including mission and information security priorities and requirements
- Collecting input from all relevant stakeholders
- Ensuring that an appropriate technical and process infrastructure is in place, including creating or modifying data collection, analysis, and reporting tools



466

467

Fig. 3. Evaluation and definition of the existing security program

### 468 **3.1.1. Gathering Stakeholder Input**

469 Gathering stakeholder input from across the organization ensures that collected measures are  
470 meaningful, yield impact and outcome findings, and provide the results necessary to address  
471 performance goals. This begins with identifying stakeholders from the top of the organizational  
472 structure and working down through organizational roles. It is important to involve a wide  
473 range of stakeholders since their interests will differ depending on what aspects of information  
474 security they interact with in their role. Each stakeholder may present a different set of  
475 measures that provide a view into their area of responsibility. Organizational elements that do  
476 not have information security as their primary responsibility but interact with information  
477 security regularly may need to be included in this process. Any organizational element  
478 responsible for measurement is also included.

479 Stakeholder interests may be determined through multiple venues, such as interviews,  
480 brainstorming sessions, mission statement reviews, in-house knowledge, and existing findings  
481 from risk assessments. There may also be laws and regulations that the organization may need  
482 to consider. Further information can be gathered by considering system-level measurement  
483 needs. Input from those who interact with individual systems and existing system-level data will  
484 provide targeted insight into the measurement needs of an organization. Ideally, stakeholder  
485 interests will be reviewed periodically during the ongoing work of the information security  
486 measurement program.

### 487 **3.1.2. Goals and Objectives**

488 Information security measurement goals and objectives are identified and documented. These  
489 may be expressed through high-level policies and requirements, laws, regulations, guidelines,  
490 and guidance. They can also be derived from organization-level goals and objectives that  
491 support the organization's mission or strategic and performance plans.

492 Applicable documents are reviewed to extract relevant information security performance goals  
493 and objectives, many of which will be identified when gathering stakeholder input. Existing  
494 metrics may also be included when identifying organizational goals and objectives. These  
495 metrics can provide valuable insight about information security, and various metrics may fit  
496 organizational needs. Newly developed goals and objectives are validated with the  
497 organizational stakeholders to ensure their understanding and support.

### 498 **3.1.3. Information Security Policies, Procedures, and Guidelines**

499 Organization-specific policies and procedures set an expectation for information security  
500 practices across all levels of the organization and typically outline details on control  
501 implementation. Applicable documents are reviewed to identify controls, processes, and  
502 performance targets. Any artifacts on information security practices are also examined when  
503 measures need to be updated or added.

#### 504 **3.1.4. Evaluating Current Implementation**

505 Any existing measures and data repositories that are used to derive measures data are  
506 reviewed to identify appropriate implementation evidence. Implementation evidence points to  
507 aspects of controls that indicate whether the information security goals and objectives are  
508 being met or whether actions that will accomplish the performance objectives in the future are  
509 being performed. The system security requirements, processes, and procedures can be  
510 extracted by consulting multiple sources, including documents, interviews, and observation.

511 Aggregating multiple system evaluations is essential for gaining a comprehensive view of an  
512 organization's security posture, including how data is collected and ingested (e.g., automated  
513 collection; consistent units, formats, and naming conventions; centralized repositories).  
514 Operationally, this will include looking at the results of regularly conducted evaluations, audits,  
515 and control and risk assessments, as well as gathering data on vulnerabilities, controls, and  
516 incident response performance. Organizations may want to combine the results of individual  
517 metrics or use scoring models to calculate their risk.

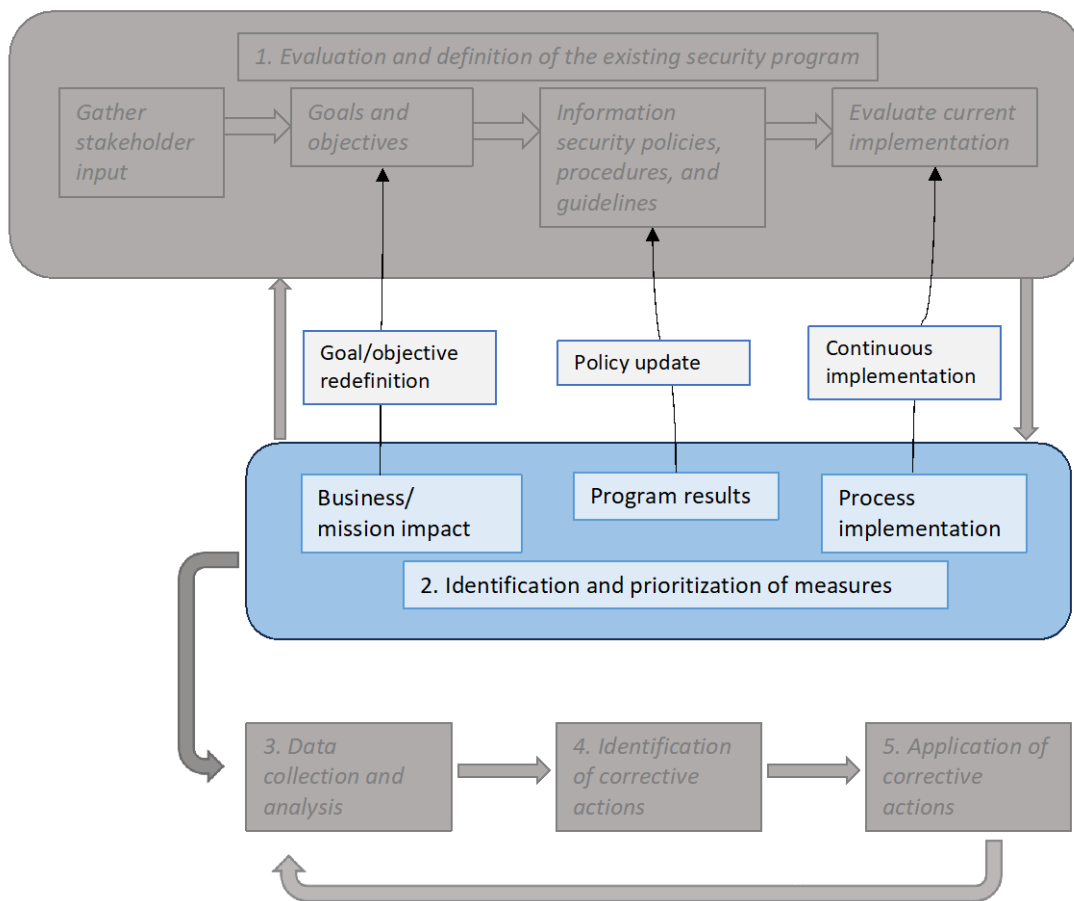
518 As system security practices evolve and the artifacts that describe them change, existing  
519 measures will be retired, and new measures will be developed. These and similar artifacts are  
520 examined to identify the new areas captured in measures and ensure that the newly developed  
521 measures are appropriate.

#### 522 **3.2. Identify and Prioritize Measures**

523 The second step in establishing an information security measurement program involves  
524 developing measures<sup>4</sup> that track process implementation, program results, and mission  
525 impacts, as shown in **Fig. 4**. The measures development tasks describe how the measures  
526 interact with the iterative process of an information security measurement program. This  
527 method of developing measures connects information security activities to the organization's  
528 strategic goals by developing and using measures that are customized to fit the organization's  
529 needs.

---

<sup>4</sup> SP 800-55v1 discusses the development and selection of specific information security measures in depth.



530

531

Fig. 4. Identify and prioritize measures

532 The existence and institutionalization of processes and procedures is foundational to the  
533 development of an information security program. As the program progresses, its policies  
534 become more detailed and better documented, the processes and procedures it uses become  
535 more standardized and repeatable, and the program can produce a greater quantity and quality  
536 of data that can be used for measurement. In this document, the categories of measures that  
537 can be collected are separated into the following three groups:

- 538
- 539 1. **Process implementation** deals with implementing measures that demonstrate the  
540 progress of specific policies, procedures, and controls. By gathering this data on  
541 implementation, an organization can see how its goals are being implemented and what  
tasks still need to be accomplished.
  - 542 2. **Program results** cover effectiveness and efficiency measures. Effectiveness measures  
543 monitor whether processes and controls are implemented, operating as intended, and  
544 meeting the desired outcome. Efficiency measures monitor the speed with which  
545 processes and controls are returning useful feedback.

546 3. **Mission impact** covers the impact measures used to articulate the impact of  
547 information security on an organization’s mission. These measures are inherently  
548 organization-specific since each organization has a unique mission. They combine  
549 information about the results of information security programs, specific controls, and  
550 associated policies and procedures implementation with various information about  
551 resources. They can also provide the most direct insight into the value of information  
552 security to the organization.

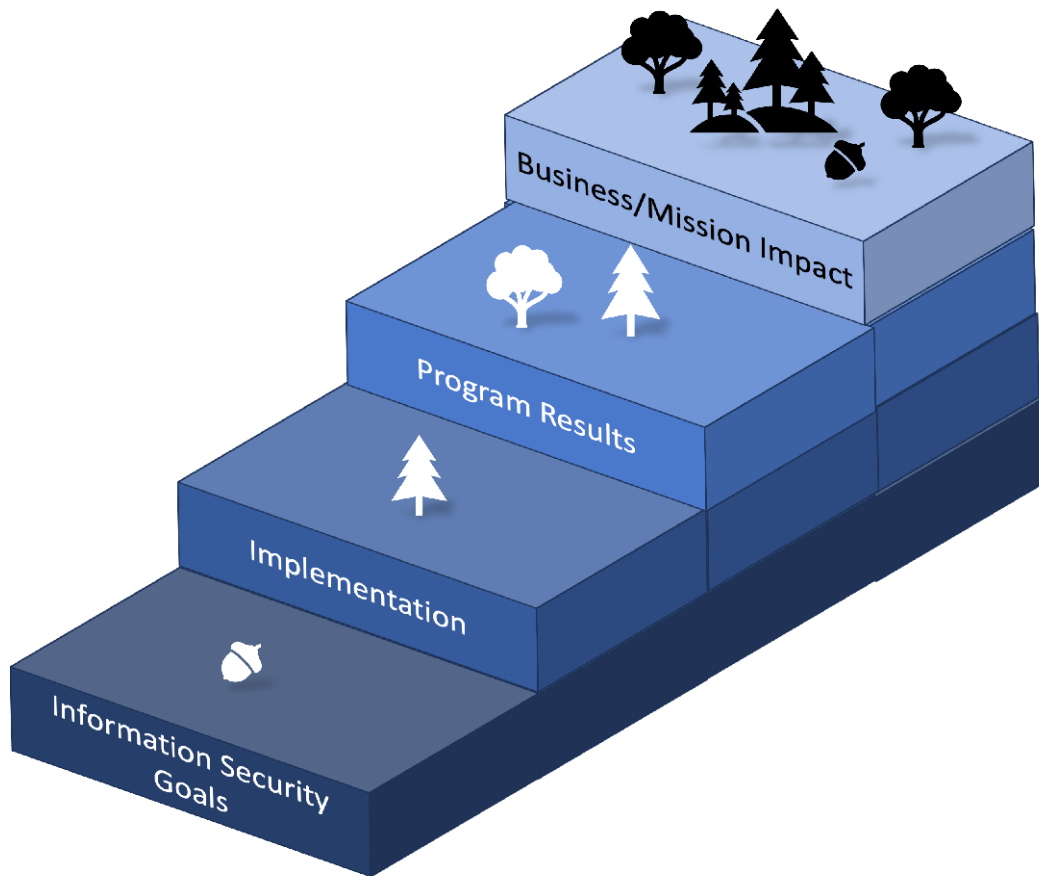
553 An organization’s ability to realistically obtain measurements in each of these categories  
554 depends on how well its security posture and information security measurement program are  
555 developed. Although different types of measures can be used simultaneously, the primary focus  
556 of information security measures shifts as the information security program continues to  
557 develop.

558 As information security program goals and strategic plans are developed, documented, and  
559 implemented, the ability to reliably collect data about the outcomes of their implementation  
560 improves.<sup>5</sup> Once information security is integrated into an organization’s processes, those  
561 processes become repeatable, measurement data collection becomes fully automated, and the  
562 mission impact of information security-related actions and events can be determined by  
563 analyzing and correlating the measurement data.

564 **Figure 5** depicts this continuum by illustrating measurement considerations for information  
565 security programs. Less mature information security programs need to develop their goals and  
566 objectives before they are able to implement effective measurements, while more mature  
567 programs use implementation measures to evaluate performance. The most mature programs  
568 use effectiveness, efficiency, and business impact measures to determine the effect of their  
569 information security processes and procedures.

---

<sup>5</sup> For many organizations, this process may be part of an Information Security Continuous Monitoring Program. In-depth information about developing an Information Security Continuous Monitoring Program Assessment can be found in SP 800-137A [1].



570

571

**Fig. 5. Information security program development and types of measurement**

572 Measures that are ultimately selected for implementation will be useful for measuring  
573 performance, identifying causes of unsatisfactory performance, pinpointing improvement  
574 areas, facilitating consistent policy implementation, effecting security policy changes, redefining  
575 goals and objectives, and supporting continuous improvement. These relationships are  
576 depicted by the feedback arrows in **Fig. 6**, which refer to:

577

578

- **Continuous implementation:** The level of implementation can provide feedback about whether the current implementation rate is appropriate.

579

580

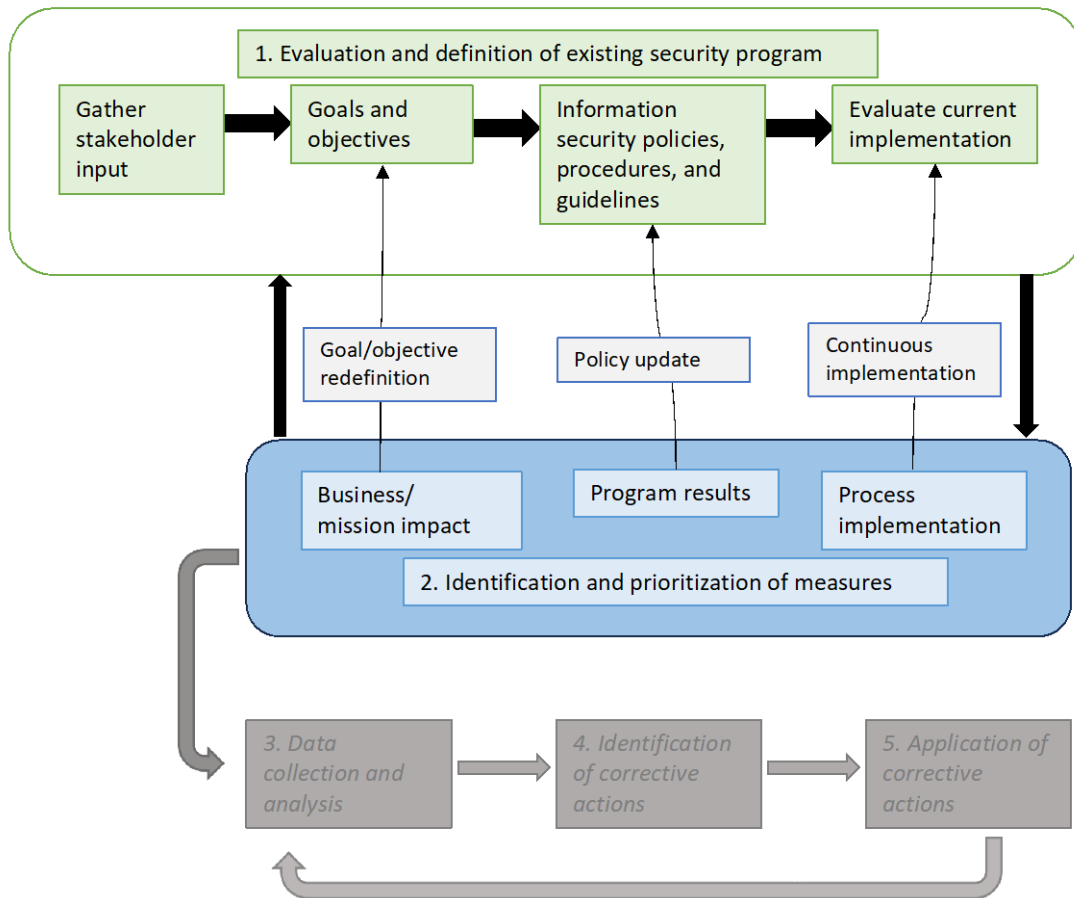
581

- **Policy update:** The feedback provided by the program results facilitate an understanding of whether the security control performance goals identified in the information security policies and procedures are realistic and appropriate.

582

583

- **Goal/objective redefinition:** Analyzing the business impact measures provides feedback that can be used when establishing organizational goals and objectives.



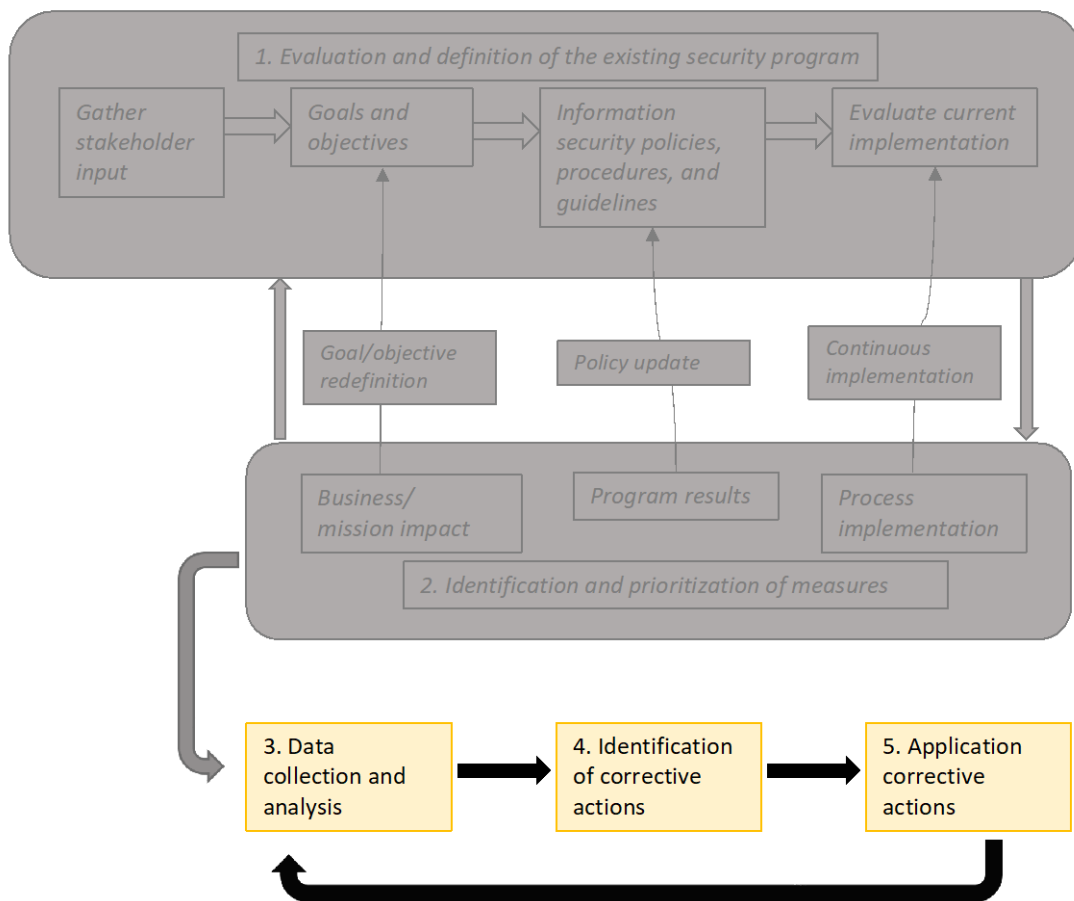
584

585

Fig. 6. Information security measures development process

### 586 3.3. Identify and Prioritize Measures

587 Information security measurement implementation involves applying measures for ongoing  
588 assessment and using the results to initiate performance improvement actions. The information  
589 security measurement program implementation process consists of three steps that — when  
590 fully executed — will ensure continuous use of these measures for security control  
591 performance monitoring and improvement. Within these three steps is a smaller loop to allow  
592 for an adaptable approach to corrective actions. The process is shown in Fig. 7.



593

594

Fig. 7. Information security measurement implementation

### 595 3.3.1. Identify and Prioritize Measures

596 Data collection and analysis involve activities that are essential for ensuring that collected  
597 measures are used to understand the organization’s information security posture and identify  
598 appropriate improvement measures:

- 599 • Collect measures data according to the processes defined in the organization’s  
600 information security measurement program Implementation process.
- 601 • Aggregate measures as appropriate to derive higher-level measures (e.g., “rolling up”  
602 system-level measures to derive program-level measures).
- 603 • Consolidate the collected data, and store it in a format conducive to data analysis and  
604 reporting (e.g., a database or spreadsheet).
- 605 • Conduct gap analysis to compare the collected measurements with targets (if defined)  
606 and identify gaps between actual and desired performance.

- 607 • Identify causes of poor performance.
- 608 • Identify areas that require improvement.

609 Using the data from more than one measure can often identify the causes of poor  
610 performance. For example, simply determining that the percentage of approved system  
611 security plans is unacceptably low would not correct the problem. The reasons for the low  
612 percentages (e.g., lack of guidelines, insufficient expertise, or conflicting priorities) are also  
613 identified. Such information can be collected as separate measures or as implementation  
614 evidence for the percentage of approved system security plans. Once this information is  
615 collected and compiled, corrective actions can be directed at the cause of the problem.

### 616 3.3.2. Identify Corrective Actions

617 Identifying corrective actions involves developing a plan for closing the implementation gap and  
618 includes the following activities:

- 619 • **Determine the range of corrective actions.** Based on results and causation factors,  
620 identify potential corrective actions for each performance issue. These may include  
621 changing system configurations; training information security staff, system  
622 administrator staff, or regular users; purchasing information security tools; changing the  
623 system architecture; establishing new processes and procedures; and/or updating  
624 information security policies.
- 625 • **Prioritize corrective actions based on overall risk mitigation goals.** Several corrective  
626 actions may apply to a single performance issue. However, some may be too costly or  
627 inconsistent with the magnitude of the problem. Applicable corrective actions are  
628 prioritized for each performance issue in ascending order of cost and descending order  
629 of impact. Corrective actions are documented for the corresponding system and tracked  
630 as a part of the continuous monitoring process.
- 631 • **Select the most appropriate corrective actions.** Viable corrective actions from the top  
632 of the prioritized list are selected for use in a full cost-benefit analysis.

633 Moving from identifying corrective actions to *applying* corrective  
634 actions may require the development of a business case and additional  
635 resources. Organizations typically have unique business case processes  
636 and life cycle spending thresholds that determine which investments  
637 and budget requests require a formal business case. In general, the  
638 level of effort to develop the business case and obtain resources  
639 corresponds with the size and scope of the funding request.

640 **3.3.3. Apply Corrective Actions**

641 Applying corrective actions involves implementing corrective actions in the security program or  
642 in the technical, management, and operational areas of controls. The plan of action and  
643 milestones (POA&M) process is used to document and monitor the corrective action status.<sup>6</sup>

644 Iterative data collection, analysis, and reporting will track the progress of corrective actions,  
645 measure improvement, and identify areas where further improvement is needed. The nature of  
646 the cycle monitors progress and ensures that corrective actions are influencing system security  
647 control implementation in the intended way. Frequent measurements will flag actions that are  
648 not implemented as planned or do not have the desired effect, enabling quick course  
649 corrections within the organization to avoid problems that could be uncovered during external  
650 audits or related activities.

651

652

---

<sup>6</sup> More information about the POA&M process can be found in SP 800-37r2.

653 **References**

- 654 [1] Dempsey K, Pillitteri V, Baer C, Niemeyer R, Rudman R, Urban S (2020) Assessing  
655 Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM  
656 Program Assessment. (National Institute of Standards and Technology, Gaithersburg,  
657 MD), NIST Special Publication (SP) 800-137A. <https://doi.org/10.6028/NIST.SP.800-137A>
- 658 [2] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk  
659 Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST  
660 Special Publication (SP) 800-30, Rev. 1. <https://doi.org/10.6028/NIST.SP.800-30r1>
- 661 [3] Joint Task Force (2018) Risk Management Framework for Information Systems and  
662 Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute  
663 of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37,  
664 Rev. 2. <https://doi.org/10.6028/NIST.SP.800-37r2>
- 665 [4] Boyens JM, Smith AM, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity  
666 Supply Chain Risk Management Practices for Systems and Organizations. (National  
667 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)  
668 800-161r1. <https://doi.org/10.6028/NIST.SP.800-161r1>
- 669 [5] Stine KM, Quinn SD, Witte GA, Gardner RK (2020) Integrating Cybersecurity and  
670 Enterprise Risk Management (ERM). (National Institute of Standards and Technology,  
671 Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286.  
672 <https://doi.org/10.6028/NIST.IR.8286>
- 673 [6] National Institute of Standards and Technology (2006) Minimum Security Requirements  
674 for Federal Information and Information Systems. (U.S. Department of Commerce,  
675 Washington, DC), Federal Information Processing Standards Publication (FIPS) 200.  
676 <https://doi.org/10.6028/NIST.FIPS.200>
- 677 [7] Software Quality Group (2021) Metrics and Measures. (National Institute of Standards  
678 and Technology, Gaithersburg, MD). Available at [https://www.nist.gov/itl/ssd/software-  
679 quality-group/metrics-and-measures](https://www.nist.gov/itl/ssd/software-quality-group/metrics-and-measures)
- 680 [8] Chew E, Swanson MA, Stine KM, Bartol N, Brown A, Robinson W (2008) Performance  
681 Measurement Guide for Information Security. (National Institute of Standards and  
682 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-55, Rev. 1.  
683 <https://doi.org/10.6028/NIST.SP.800-55r1>

684 **Appendix A. Glossary**

685 **assessment**

686 The action of evaluating, estimating, or judging against defined criteria. Different types of assessment (i.e.,  
687 qualitative, quantitative, and semi-quantitative) are used to assess risk. Some types of assessment yield results.

688 **assessment results**

689 The output or outcome of an assessment.

690 **information security**

691 The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or  
692 destruction to provide confidentiality, integrity, and availability. [6]

693 **key performance indicator**

694 A metric of progress toward intended results.

695 **key risk indicator**

696 A metric used to measure risk.

697 **mean time to detect**

698 A metric that tracks the average amount of time that a problem exists before it is found.

699 **mean time to recovery**

700 A metric that tracks the average amount of time that it takes to recover from a product or system failure.

701 **measurement**

702 The process of obtaining quantitative values using quantitative methods.

703 **measures**

704 Quantifiable and objective values that result from measurement.

705 **metrics**

706 Measures and assessment results designed to track progress, facilitate decision-making, and improve performance  
707 with respect to a set target.

708 **qualitative assessment**

709 The use of a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels. [7]

710 **quantitative assessment**

711 The use of a set of methods, principles, or rules for assessing risk based on numbers where the meanings and  
712 proportionality of values are maintained inside and outside of the context of the assessment. [7]

713

714 **Appendix B. Change Log**

715 *[Upon final publication, a change log will be included that describes differences from the*  
716 *superseded version of this publication: NIST SP 800-55r1 (2008).]*

717 In <date of final publication> the following changes were made to the report:

- 718     • ...

719