NIST Special Publication 800
NIST SP 800-55v2

# Measurement Guide for Information Security

*Volume 2 — Developing an Information Security Measurement Program*

Katherine Schroeder
Hung Trinh
Victoria Yan Pillitteri

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

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

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

# Measurement Guide for Information Security

*Volume 2 — Developing an Information Security Measurement Program*

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

December 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 2024-11-04
Supersedes NIST SP 800-55 Rev. 1 (July 2008) https://doi.org/10.6028/NIST.SP.800-55r1

**How to Cite this NIST Technical Series Publication**
Schroeder K, Trinh H, Pillitteri VY (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. https://doi.org/10.6028/NIST.SP.800-55v2

**Author ORCID iDs**
Katherine Schroeder: 0000-0002-4129-9243
Hung Trinh: 0000-0002-3323-0836
Victoria Yan Pillitteri: 0000-0002-7446-7506

**Contact Information**
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

**Additional Information**
Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/55/v2/final, including related content, potential updates, and document history.

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

**Abstract**

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

**Keywords**

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

**Reports on Computer Systems Technology**

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

**Audience**

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

**Patent Disclosure Notice**

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

## Table of Contents

## List of Figures

# 1. Introduction

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

## 1.1. Purpose and Scope

NIST Special Publication (SP) 800-55v2 (Volume 2) is a flexible guide for developing and implementing an information security measurement program. The term "program" in SP 800-55v2 is intended to signify a flexible structure for approaching activities around the development and implementation of information security measures. A measurement program can be part of an existing cybersecurity program or its own dedicated effort. Measures provide the means for tying information security policy, procedure, and control[1] implementation, efficiency, and effectiveness to an organization's success in its business activities.

This document provides a methodology for developing and implementing an information security measurement program, while SP 800-55v1 [10] addresses the selection and development of information security measures. SP 800-55v2 discusses the concept of organizational or program maturity but is not intended for use as a maturity model and is intentionally agnostic toward any specific maturity models.

## 1.2. Relationship to Other NIST Publications

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

- SP 800-137A, *Assessing Information Security Continuous Monitoring Programs* [1]
- *The NIST Cybersecurity Framework (CSF) 2.0* [2]
- SP 800-30r1 (Revision 1), *Guide for Conducting Risk Assessments* [3]
- SP 800-37r2, *Risk Management Framework for Information Security Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [4]
- SP 800-161r1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* [5]
- Internal Report (IR) 8286, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management (ERM)* [6]

[1] This document uses the term *controls* to broadly describe identified countermeasures for managing information security risks. It is intended to be framework- and standard-agnostic and can also apply to other existing models or frameworks.

## 1.3. Document Organization

The remaining sections of this document discuss the following:

- Section 2, Fundamentals
- Section 3, Workflow for Implementing an Information Security Measurement Program
- Appendix A, Glossary
- Appendix B, Change Log

## 1.4. Document Terminology

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

- **Assessment:** The action of evaluating, estimating, or judging against defined criteria. Different types of assessment (i.e., qualitative, quantitative, and semi-quantitative) are used to assess risk. Some types of assessment yield measures.
- **Assessment result:** The output or outcome of an assessment.
- **Controls:** Used here to broadly to describe identified countermeasures to manage information security risks.
- **Information security**[2]**:** The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. [7]
- **Measurement:** The process of obtaining quantitative values using quantitative methods.
- **Measures:** Quantifiable and objective values that result from measurement.
- **Metrics:** Measures and assessment results designed to track progress, facilitate decision-making, and improve performance with respect to a set target.
- **Program:** A flexible structure for approaching activities around the development and implementation of cybersecurity measures.
- **Qualitative assessment:** The use of a set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels. [3]
- **Quantitative assessment:** The use of a set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside of the context of the assessment. [3]
- **Semi-quantitative assessment:** The use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. [3]

[2] The term “cybersecurity” can be used interchangeably with “information security.”

## 2. Fundamentals

A comprehensive information security measurement program provides evidence to support decisions that directly affect the information security posture of an organization, including budget and personnel requests and the allocation of available resources. A measurement program evaluates the existing security program, identifies and prioritizes potential measures, and implements a structure for collecting data and applying corrective actions based on the findings of those measures. Having a structure to develop and implement information security measures allows for a repeatable and archivable process. An information security measurement program can also support reporting requirements related to information security performance. A relevant measurement program needs support from across the organizational structure.

### 2.1. Measurement Program Benefits

A measurement program can provide a consistent and defined structure for collecting, analyzing, and communicating about data to monitor information security risks. It is crafted to meet an organization's specific risk management goals and legal or regulatory requirements and to enable data-driven decisions about information security. The data collected through a measurement program can help organizations understand how well they are managing their information security risks, whether their personnel are sufficiently educated and trained to minimize risks to the organization, and whether a new service or technology might better serve their security posture. A defined and consistent measurement program enables discussions and communication around measures and the goals of measurement. Where measures and metrics provide data, the program itself provides a broader context and lens to consistently interpret, analyze, and communicate the larger impacts of information security measures.

An information security measurement program can increase accountability by helping organizations identify if specific controls that are implemented correctly, are not implemented, or are ineffective. The continuous feedback provided by a structured measurement program supports regular internal communications that collect data about information security performance and risks for high-level members of the organization. Implementing an information security measurement program demonstrates an organizational commitment to proactive information security and continuous improvement. For example, organizations that use the Cybersecurity Capacity Maturity Model (CMM) may implement a measurement program as part of the goal of demonstrating the Level 4, "Managed," degree of performance. When using the appropriate measures, an information security measurement program enables organizations to quantify improvements in securing systems and demonstrate quantifiable progress in accomplishing strategic goals and objectives. More information on selecting measures can be found in SP 800-55v1.

### 2.2. Program Scope

To ensure the success of program-level measurement, the organization needs consistent, repeatable processes and data availability across the enterprise. In a successful measurement program, these processes are customized to the different environments and needs of the

individual organization. Measures can be applied to organizational units, sites, or other constructs to meet specific stakeholder requirements, strategic goals, operating environments, risk priorities, and information security program maturity.

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

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

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

1. Strong upper-level management support that is integrated into the culture of the organization
2. Practical information security policies and procedures
3. Applicable, quantifiable measures
4. Results-oriented measures analysis

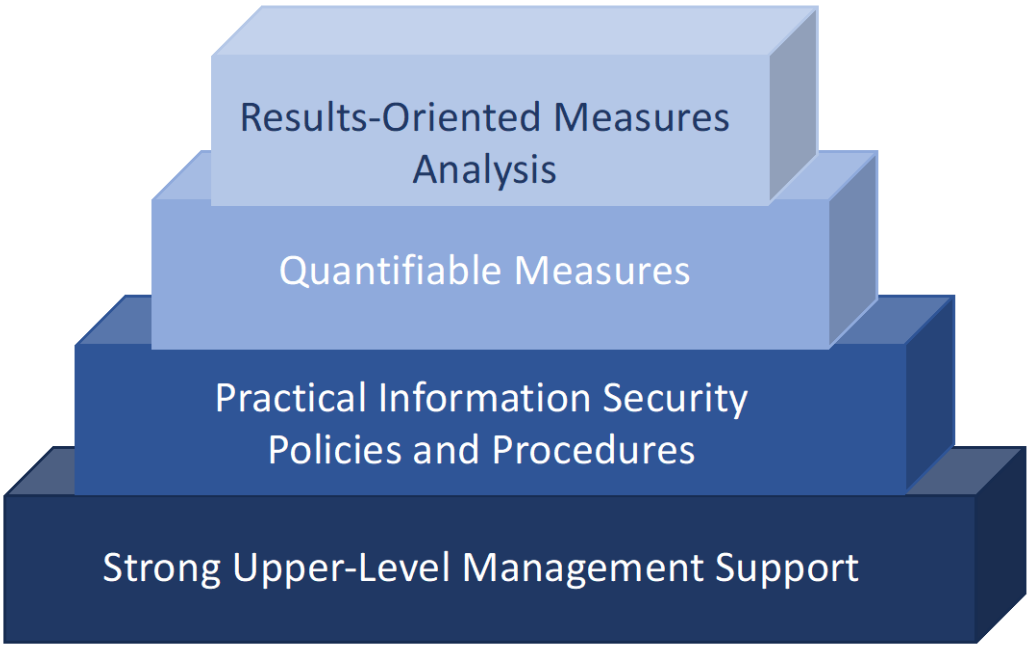


**Fig. 1. Information security measurement program structure**

A foundation of strong upper-level management support that is integrated into organizational culture is critical to the success of an information security program. This support establishes a focus on information security within the highest levels of the organization and continues throughout the organization. An information security measurement program can fail under the pressure of organizational dynamics and budget limitations without the proactive support of personnel in positions that control resources.

An effective information security measurement program has practical information security policies and procedures backed by the authority necessary to enforce compliance and manage risk. Information security policies define the information security management structure, assign information security responsibilities, and reliably measure progress. The related procedures document management's position on implementing information security controls and the rigor with which they are applied. Measures are not easily obtainable if there are no procedures to supply data for measurement.

Quantifiable measures based on performance objectives are developed and established to provide meaningful performance data. Successful security measures are applicable to the organization's risk management goals and align with organizational requirements. The goals of these measure are to be easily obtainable, feasible to measure, and repeatable to show relevant performance trends, track performance, and direct resources.

Finally, the information security measurement program emphasizes consistent and periodic analyses of the data provided by measurements, which allows for security issues to be

addressed. The lessons learned from these analyses can improve the effectiveness of existing controls and help organizations plan the implementation of future controls. To ensure meaningful and useful collected data, stakeholders and users will prioritize accurate data collection. More information on quantifiable measures and measures analysis can be found in SP 800-55v1.

## 2.4. Roles and Responsibilities

This section outlines the key roles and responsibilities for developing and implementing an information security measurement program. While all organization members are ultimately responsible for information security, the positions described here are specific to key information security stakeholders. Organizations have varying missions, business functions, and organizational structures, so there may be differences in naming conventions and how responsibilities are allocated across organizational personnel. However, known functions and responsibilities must be assigned to ensure accountability. To achieve desired outcomes, all roles must be empowered and resourced, regardless of the organizational structure adopted. The application of a measurement program as described in this publication is intended to be flexible and allow organizations to manage their measurement needs.

### 2.4.1. Chief Executive Officer/Agency Head

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

- Ensuring that information security measures are used in support of strategic and operational planning processes to secure the organization's mission
- Ensuring that the Chief Information Officer (CIO) or Chief Information Security Officer (CISO) integrates information security measures into annual reporting on the effectiveness of the information security program
- Demonstrating support for information security measures development and implementation and communicating official support to the organization
- Providing adequate financial and human resources for successful information security measurement activities
- Actively promoting information security measurement as an essential facilitator of information security performance improvement throughout the organization
- Approving policies to officially institute measures collection

### 2.4.2. Chief Information Officer[3]

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

- Orchestrating the development and implementation of an information security measurement program
- Using information security measures to assist in monitoring compliance with applicable information security requirements
- Using information security measures to report on the effectiveness of the organization's information security program
- Demonstrating management's commitment to the development and implementation of information security measures through formal leadership
- Formally communicating the importance of using information security measures to monitor the overall health of the information security program and comply with applicable regulations
- Allocating adequate and consistent financial and human resources to the information security measurement program
- Regularly reviewing information security measures and using that feedback to support policies, resource allocation, budget decisions, and assessments of the information security program's posture and operational risks to agency information systems
- Ensuring that a process is in place to prioritize and address issues discovered through measures analysis and taking corrective actions, such as revising information security procedures and providing additional information security training to staff
- Explicitly assigning specific individuals with the necessary authority and resources to remediate exceptions identified by the information security measurement program
- Approving and issuing policies, procedures, and guidelines to officially develop, implement, and institute measures

### 2.4.3. Chief Information Security Officer

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

- Implementing information security measures address information security risks and provide the resolution needed by the organization's overall risk management goals
- Integrating information security measurement into the process for planning, implementing, evaluating, and documenting remedial actions to address any

[3] When a federal agency has not designated a formal CIO position, FISMA requires the associated responsibilities to be handled by a comparable agency official.

deficiencies in the organization's information security policies, procedures, and practices

- Obtaining adequate financial and human resources to support the development and implementation of an information security measurement program
- Leading the development of internal guidelines or policies related to information security measures
- Utilizing information security measures to report on the effectiveness of the organization's information security program, including remedial actions
- Ensuring that a standard process is used throughout the organization for information security measures development, creation, analysis, and reporting
- Using information security measures for policy, resource allocation, and budget decisions

### 2.4.4. Program Managers and System Owners

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

- Participating in information security measurement program development and implementation by providing feedback on the feasibility of data collection and identifying data sources and repositories
- Implementing corrective actions identified through measuring information security
- Educating staff on the development, collection, analysis, and reporting of information security measures and their effects on information security policy, requirements, resource allocation, and budget decisions
- Confirming that measurement data is consistently and accurately collected and provided to designated staff for analysis and reporting
- Directing the full participation and cooperation of staff, when required
- Regularly reviewing information security measures data and using the data for policy, resource allocation, and budget decisions
- Supporting the implementation of corrective actions identified by measuring information security performance

### 2.4.5. Other Roles

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

- Participating in the development and implementation of an information security measurement program by providing feedback on the feasibility of data collection and identifying data sources and repositories
- Collecting data or providing measurement data to designated staff who are collecting, analyzing, and reporting data
- Partnering with technology, architects, engineers, and operations teams to ensure that technology is selected, configured, and deployed to deliver the metrics requires by the information security measurement program

Information security measurement may require additional input and coordination from various organizational components or stakeholders, including incident response, information technology operations, privacy, enterprise architecture, human resources, physical security, legal counsel, and others.

## 2.5. Programmatic Value of Metrics

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

By keeping metrics consistent over time, a measurement program can evaluate long-term trends and expected ranges. A new metric may provide important insights, but tracking the measurements related to metrics over a continuous period (e.g., quarter to quarter, year to year) will give more information about the success of organization-, program-, and system-level information security plans, policies, procedures, and goals. Metrics enable goal-setting against industry standards and internal targets. An organization may find a wide variety of metrics to fit their needs, and by utilizing the findings of an information security measurement program, the organization will be better prepared to make decisions about measures and track changes. More information about the process of selecting and analyzing specific measures can be found in SP 800-55v1.

## 2.6. Measures Communication

An information security measurement program plays a crucial role in enhancing organizational communication and providing insights to higher-level management and executives. A major challenge concerning information security measurement is translating technically measurable performance data into a form that is contextually relevant to the consumer of the report.

Measurements provide quantifiable data about an organization’s information security posture, such as incident response times. This data can then be used to make informed decisions about resource allocation, risk mitigation strategies, and investment priorities. Senior leadership will consider their organization’s reporting requirements to identify the most useful reporting style.

Data from various sources (e.g., vulnerability scans, incident logs, and compliance assessments) can be aggregated to help executives understand information security. Summarizing measurement findings and metrics into concise reports facilitates efficient communication. Regularly reporting on measurement and assessment results fosters transparency, promotes accountability for meeting performance targets, and encourages continuous improvements. Sharing findings with executives demonstrates the organization's commitment to its information security posture.

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

- What measures tell a more precise risk story?
- What measures would drive necessary action?
- What measures will be best understood by the recipient?
- What measures deliver risk insights most effectively?

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

Communication about information security measures can be narrow or broad, casual or formal. For example, short memos may respond to direct questions and only show one or two measures, whereas a formal annual report may include more detailed information about the organization's information security posture, risks, audits, confirmed findings, and compliance. A more detailed annual report will require measures related to all of the topics covered in the report. The specific needs and reporting structure of a request for information will determine what data be reported on.

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

## 2.7. Measurement Program Considerations

When an organization is building a measurement program, the consideration of the specific organizational structure, processes, required budget, personnel, and time resources help make the program successful.

### 2.7.1. Organizational Considerations

The development and implementation of information security measures will be coordinated with appropriate stakeholders from relevant organizational elements. Include those who regularly interact with information security even if it is not their primary responsibility, such as the training, resource management, and legal departments. The program will also comply with any existing processes for approving organization-wide data calls and actions. Effective coordination among different organizational elements can ensure that information security measures are implemented uniformly across the organization.

### 2.7.2. Manageability

Organizations need to be able to manage their information security measurement program. Here, "manageability" refers to having the organizational resources to support the measurement program's goals and objectives. The results of many information security activities can be quantified and used for measurement. However, since resources are limited, organizations prioritize measurement requirements to ensure that a limited number of measures are gathered. Ensuring that each stakeholder is responsible for as few measures as possible may make the collected measures meaningful, yield impact and outcome findings, and provide stakeholders with the time necessary to address performance gaps. As the program continues to develop and target levels of measurement are reached, obsolete measures are phased out, and new measures that show the completion and effectiveness of more current items are used.[4] Further measures will also be required if the organization's mission is redefined or if changes are made to information security policies and guidelines.

### 2.7.3. Data Management Concerns

Having an information security measurement program in place helps organizations establish consistent and well-defined methods for collecting security-related data, including defining what data to collect, how to collect, and at what intervals. Operationally, this may include identifying relevant data sources, determining granularity, and validating data accuracy. The information security measurement program can also ensure that clear metadata is used by defining how data will be normalized with consistent units and formats for accurate aggregation and meaningful comparison. As effective reporting processes are aligned with the information security measurement program's goals, taking the time to establish a consistent data management environment provides a solid foundation for gathering and aggregating measures data. Lastly, when collecting and storing measurement data, protect the data at the same level as the system itself.

[4] 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.

## 3. Workflow for Implementing an Information Security Measurement Program

The workflow of implementing an information security measurement program consists of five major activities, as shown in Fig. 2:

1. Evaluation and definition of the existing security program
2. Identification and prioritization of measures
3. Data collection and analysis
4. Identification of corrective actions
5. Application of corrective actions

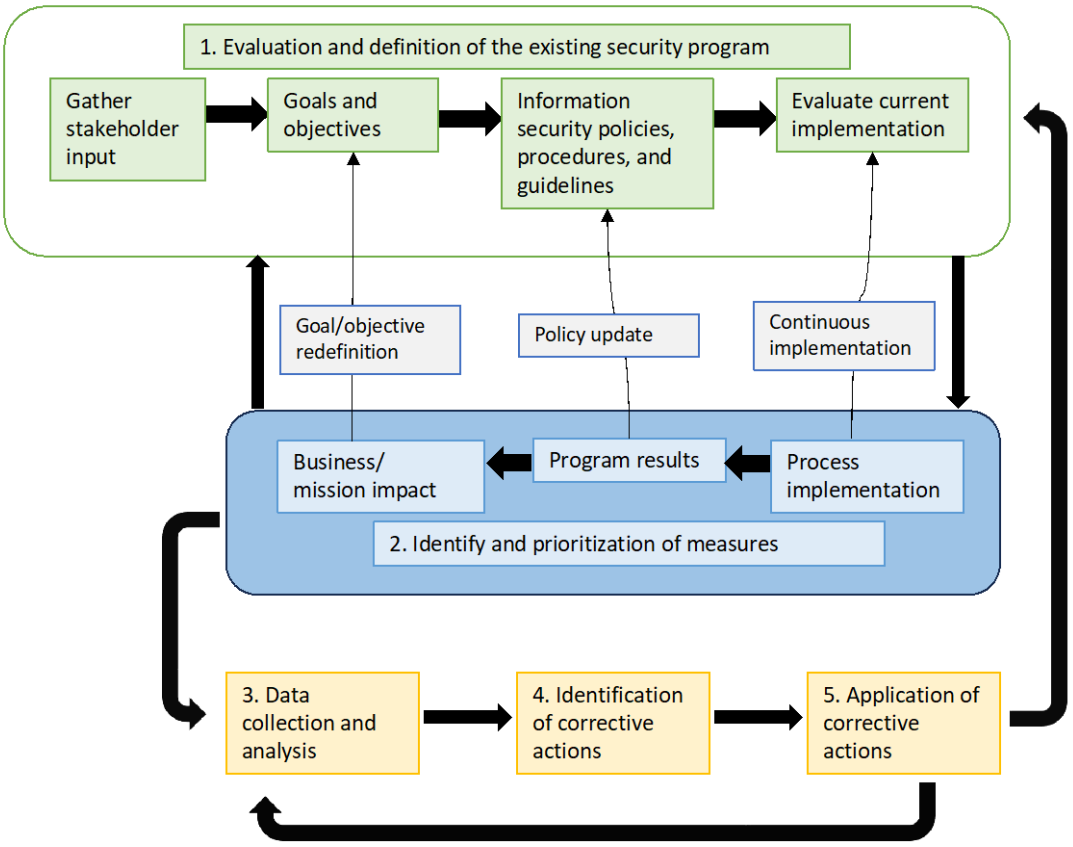


**Fig. 2. Information security measurement program workflow**

The process is provided in a linear form to encourage the use of a consistent yet flexible methodology that can be tailored to a specific organization and its unique stakeholder groups

and applied across different levels of the organization. While the tasks outlined in Fig. 2 appear in sequential order, the process of implementing an information security measurement program may vary by organization and require iterative cycles between task execution and revisiting tasks. There may also be other opportunities to diverge from the sequential nature of the tasks when it is more effective, efficient, or cost-effective to do so.

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

When building and maintaining an information security measurement program, organizations will first identify their measurement needs, as shown in Fig. 3.

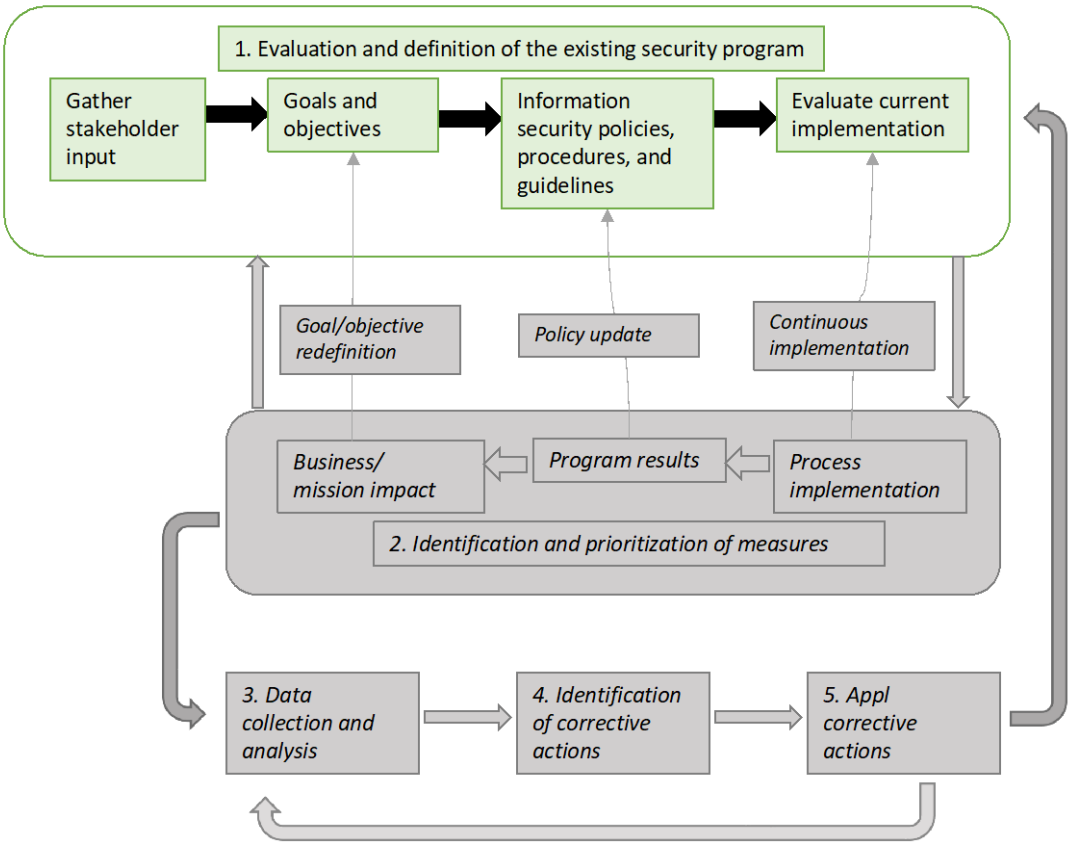


**Fig. 3. Evaluation and definition of the existing security program**

Ultimately, there is value in having both stability and flexibility in selecting organizational measures. Important considerations for measurement programs include:

- Selecting 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

### 3.1.1. Gathering Stakeholder Input

Gathering stakeholder input from across the organization ensures that collected measures are meaningful, yield impact and outcome findings, and provide the results necessary to address performance goals. This begins with identifying stakeholders from the top of the organizational structure and working down through organizational roles. It is important to involve a wide range of stakeholders since their interests will differ depending on what aspects of information security they interact with in their roles. Individual organizations will determine which stakeholders to involve and how and when to include them. Each stakeholder may present a different set of measures that provide a view into their area of responsibility. Organizational elements that do not have information security as their primary responsibility but interact with information security regularly may need to be included in this process. While organizational elements that are responsible for measurement are also included, it may not be possible to acquire, process, and implement all stakeholder input, depending on the size of the organization.

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

### 3.1.2. Goals and Objectives

Information security measurement goals and objectives are identified and documented. Organizational measurement goals and objectives are implicitly tied to their ability to mitigate or reduce threats and risks. As the threat or risk landscape evolves, goals and measures may need to adapt accordingly. These goals and objectives may be expressed through high-level policies and requirements, laws, regulations, guidelines, and guidance. They can also be derived from organization-level goals and objectives that support the organization's mission or strategic and performance plans.

Applicable documents and existing metrics can provide valuable insight about information security, and various metrics may fit organizational needs. Newly developed goals and objectives are validated with the organizational stakeholders to ensure their understanding and support.

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

Organization-specific policies and procedures set an expectation for information security practices across all levels of the organization and typically outline details on control implementation. Applicable documents are reviewed to identify controls, processes, and performance targets. Any artifacts on information security practices are also examined when measures need to be updated or added. As policies, procedures, and guidelines tie into broader risk management procedures, some organizations may need to meet high-level governance expectations when evaluating and executing control implementation.

### 3.1.4. Evaluating Current Implementation

Any existing measures and data repositories are reviewed to identify implementation evidence that indicates whether the information security goals and objectives are being met or whether actions that will accomplish the performance objectives in the future are being performed. The level of effort, subjectivity, and the difficulty of assessment are necessary considerations when implementing measures. Often, the best implementation evidence can be resolved with a binary answer, such as “yes/no” or “pass/fail.” The system security requirements, processes, and procedures can be extracted by consulting multiple sources, including documents, interviews, and observation.

Aggregating multiple system evaluations is essential to gaining a comprehensive view of an organization’s security posture, including how data is collected and ingested (e.g., automated collection; consistent units, formats, and naming conventions; centralized repositories). Operationally, this will include analyzing the results of regularly collected control implementation metrics or time-series evaluations, audits, and control and risk assessments, as well as gathering data on vulnerabilities, controls, and incident response performance. Organizations may want to combine the results of individual metrics or use scoring models to calculate their risk.

As system security practices evolve and the artifacts that describe them change, existing measures will be retired, and new measures will be developed. These and similar artifacts are examined to identify the new areas captured in measures and ensure that the newly developed measures are appropriate. Thus, the organization may establish a mechanism to review information security measures:

- On a regular basis
- In response to any impactful event (e.g., by identifying all of the existing measures that could have predicted an issue, identifying any missing measures that could be implemented to improve organizational visibility of risks)

## 3.2. Identification and Prioritization of Measures

The second step in establishing an information security measurement program involves developing measures[5] that track process implementation, program results, and mission impacts, as shown in Fig. 4.

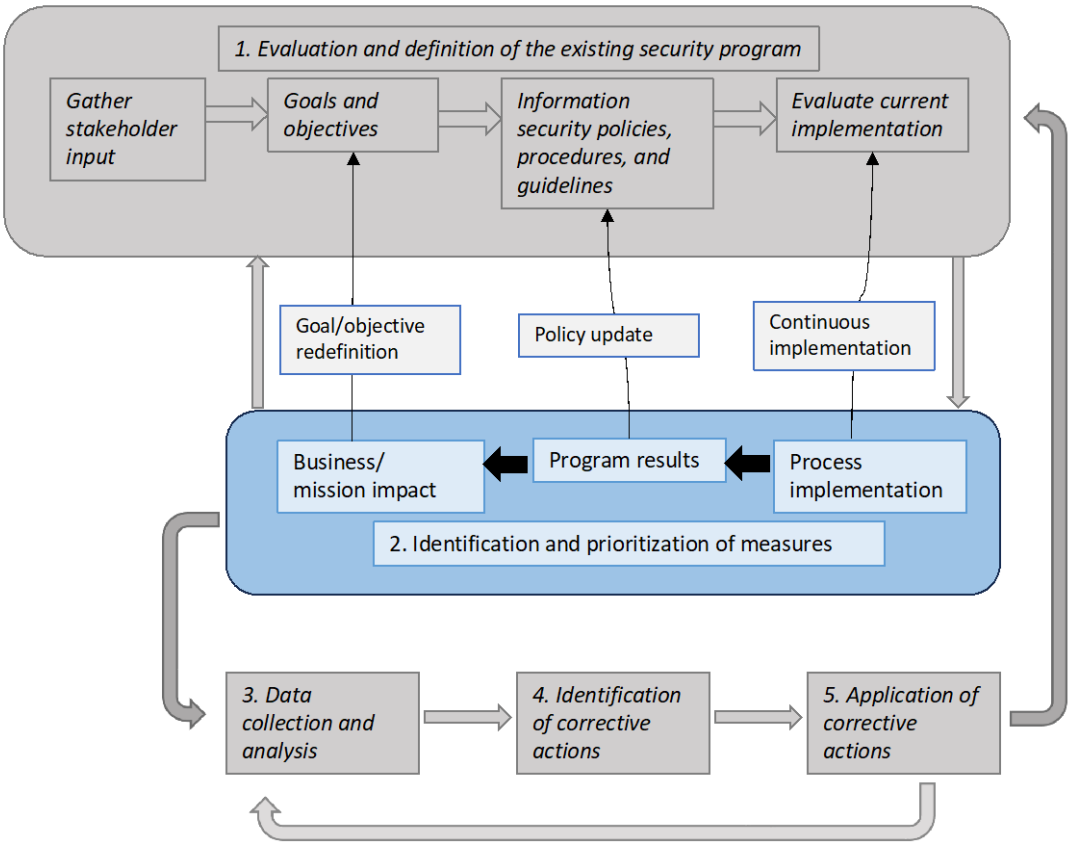


**Fig. 4. Identify and prioritize measures**

The measures development tasks describe how the measures interact with the iterative process of an information security measurement program. This method connects information security activities to the organization's strategic goals by developing and using measures that are customized to fit the organization's needs.

The existence and institutionalization of processes and procedures are foundational to the development of an information security program. As the program progresses, its policies become more detailed and better documented, the processes and procedures it uses become

[5] SP 800-55v1 discusses the development and selection of specific information security measures in depth.

more standardized and repeatable, and the program can produce a greater quantity and quality of data for measurement. In this document, the categories of measures that can be collected are separated into the following three groups:

1. **Process implementation** deals with implementing measures that demonstrate the progress of specific policies, procedures, and controls. By gathering this data on implementation, an organization can see how its goals are being implemented and what tasks still need to be accomplished.
2. **Program results** cover effectiveness and efficiency measures. Effectiveness measures monitor whether processes and controls are implemented, operating as intended, and meeting desired outcomes. Efficiency measures monitor the speed with which processes and controls return useful feedback.
3. **Mission impact** covers the impact measures used to articulate the impact of information security on an organization's mission. These measures are inherently organization-specific since each organization has a unique mission. They combine information about the results of information security programs, specific controls, and associated policies and procedures implementation with various information about resources. They can also provide the most direct insight into the value of information security to the organization.

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

As information security program goals and strategic plans are developed, documented, and implemented, the ability to reliably collect data about the outcomes of their implementation improves.[6] Once information security is integrated into an organization's processes, those processes become repeatable, measurement data collection becomes fully automated, and the mission impact of information security-related actions and events can be determined by analyzing and correlating the measurement data.

When an information security measurement program is first introduced, the focus will be on ensuring that the information security objectives of the organization are met through implementation, coverage, functionality, or capability. As improvements are made and information security goals are mostly or fully met, the emphasis on measurement can be migrated toward efficiency, effectiveness, and business impacts. Organizations determine the appropriate types of measurement that they are gathering to ensure that they meet organizational goals and are feasible to implement. Figure 5 depicts this continuum by illustrating measurement considerations for information security programs.

[6] For many organizations, this process may be part of an Information Security Continuous Monitoring Program, which is discussed in-depth in SP 800-137A [1].

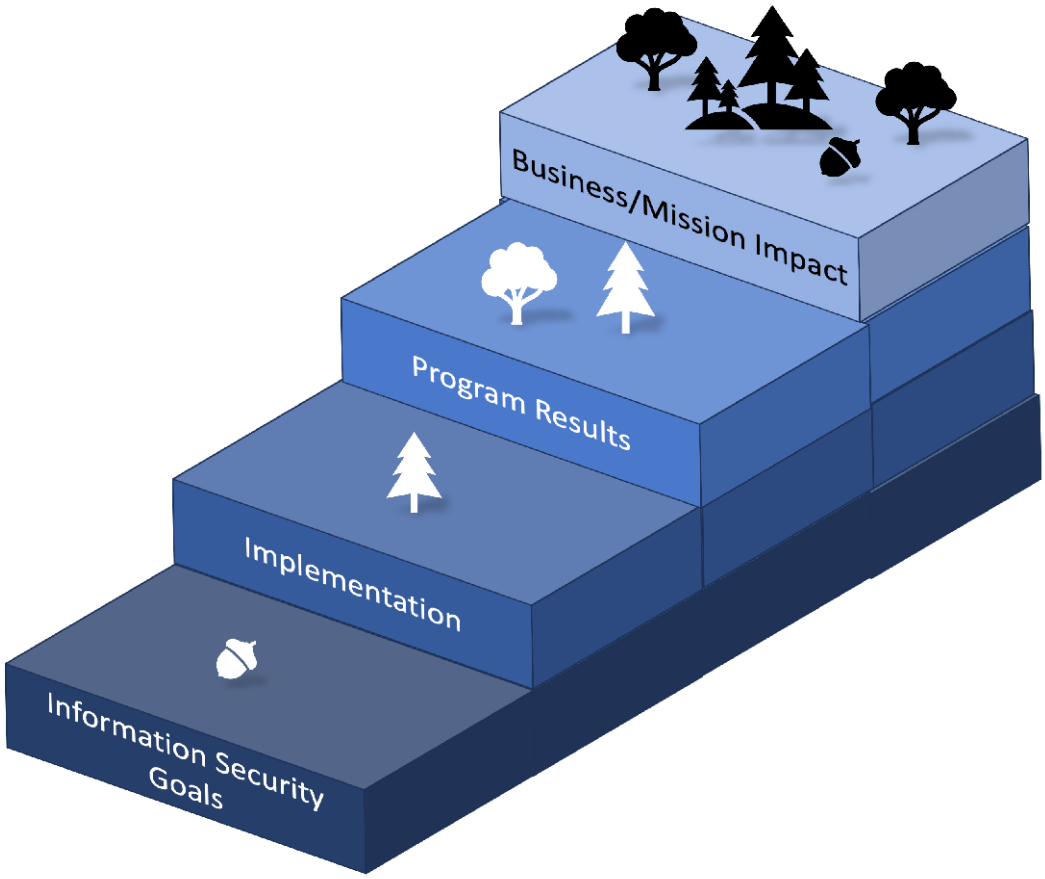


**Fig. 5. Information security program development and types of measurement**

Measures that are ultimately selected for implementation will identify causes of unsatisfactory performance, pinpoint improvement areas, facilitate consistent policy implementation, affect security policy changes, redefine goals and objectives, and support continuous improvement. These relationships are depicted by the feedback arrows in Fig. 6, which refer to:

- **Continuous implementation:** The level of implementation can provide feedback about whether the current implementation rate is appropriate.
- **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.
- **Goal/objective redefinition:** Analyzing the business impact measures provides feedback that can be used when establishing organizational goals and objectives.

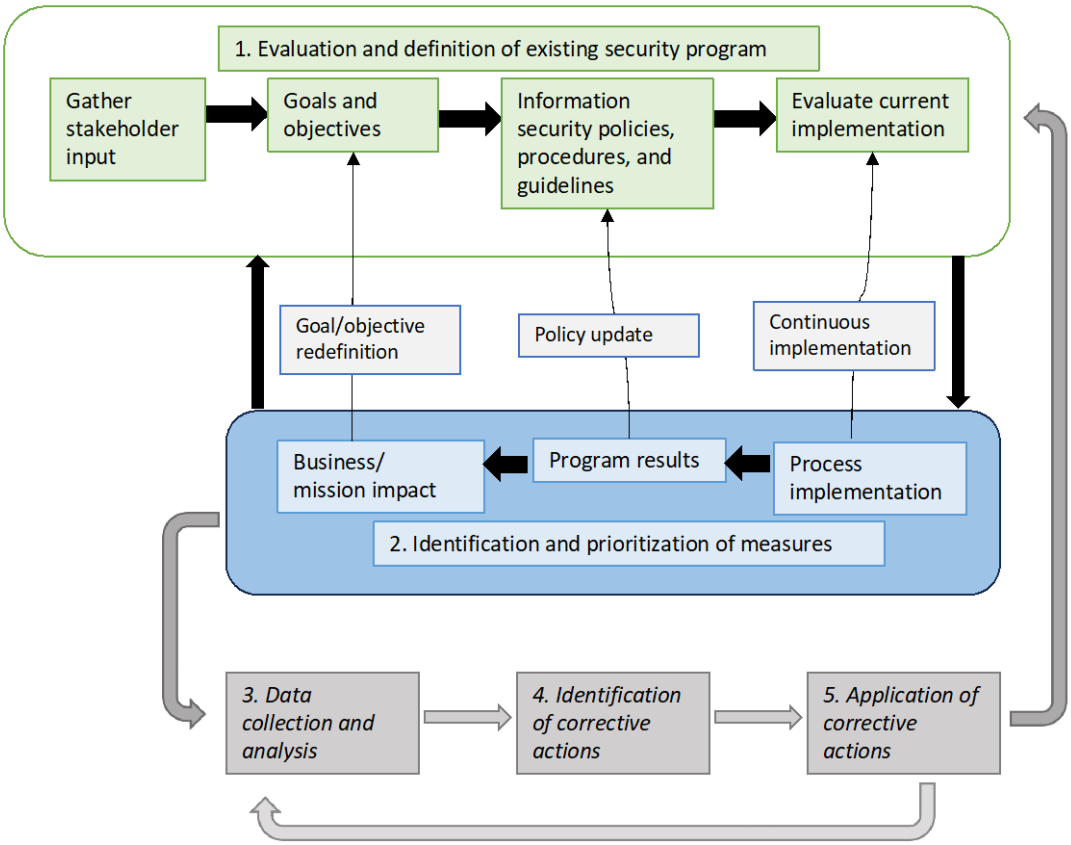


**Fig. 6. Information security measures development process**

## 3.3. Data Collection and Analysis

Information security measurement implementation consists of three steps for monitoring and improving performance, including a smaller loop to allow for an adaptable approach to corrective actions. The process is shown in Fig. 7.

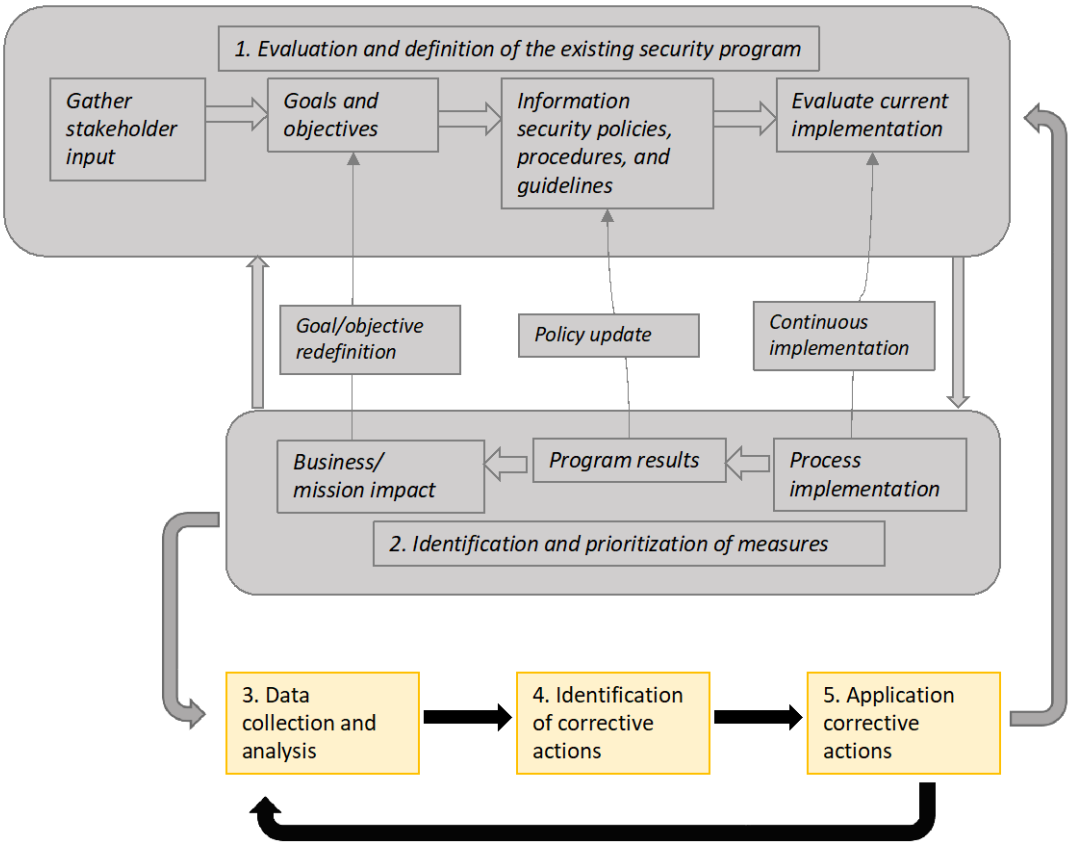


**Fig. 7. Information security measurement implementation**

Data collection and analysis involve essential activities for understanding the organization's information security posture and identifying appropriate improvement measures:

- Collect measures data according to the processes defined in the organization's information security measurement program implementation process.
- Aggregate measures as appropriate to derive higher-level measures (e.g., "rolling up" system-level measures to derive program-level measures).
- Consolidate the collected data and store in a format that is conducive to data analysis and reporting (e.g., a database or spreadsheet).
- Conduct gap analysis to compare the collected measurements with targets (if defined) and identify gaps between actual and desired performance.

- Identify causes of poor performance.
- Identify areas that require improvement.

In the early stages of an information measurement program, organizations may find it helpful to have a larger pool of measures to identify those that provide the most useful feedback, especially if the organization lacks the resources to actively monitor and assess all potential data points. As more accurate and relevant measures and data sources are identified and capabilities improve, an organization may be able to narrow the harvested data points to the most useful areas for analysis.

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

### 3.4. Identify Corrective Actions

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

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

> *Applying* corrective actions may require the development of a business case and additional resources. Organizations typically have unique business case processes and life cycle spending thresholds that determine which investments and budget requests require a formal business case. In general, the level of effort to develop the business case and obtain resources corresponds with the size and scope of the funding request.

### 3.5. Apply Corrective Actions

Corrective actions are applied in the security program or in the technical, management, and operational areas of controls. The plan of action and milestones (POA&M) process is used to document and monitor the corrective action status.[7]

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

[7] More information about the POA&M process can be found in SP 800-37r2.

## References

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

[2] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

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

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

[5] Boyens JM, Smith AM, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-161r1-upd1, Includes updates as of November 1, 2024 . https://doi.org/10.6028/NIST.SP.800-161r1

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

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

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

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

[10] Schroeder K, Trinh H, Pillitteri VY (2024) Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-55v1. https://doi.org/10.6028/NIST.SP.800-55v1

## Appendix A. Glossary

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

**assessment results**
The output or outcome of an assessment.

**information security**
The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. [7]

**key performance indicator**
A metric of progress toward intended results.

**key risk indicator**
A metric used to measure risk.

**mean time to detect**
A metric that tracks the average amount of time that a problem exists before it is found.

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

**measurement**
The process of obtaining quantitative values using quantitative methods.

**measures**
Quantifiable and objective values that result from measurement.

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

**qualitative assessment**
The use of a set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels. [8]

**quantitative assessment**
The use of a set of methods, principles, or rules for assessing risk based on numbers where the meanings and proportionality of values are maintained inside and outside of the context of the assessment. [8]

## Appendix B. Change Log

In December 2024, the following changes were made to this Special Publication:

- Separated document into two volumes. Volume 1 focuses on identifying and selecting measures, and Volume 2 focuses on developing a measurement program
- The information originally found Sec. 2, Roles and Responsibilities, has been updated and can now be found in Sec. 2.4.
- The information originally found Sec. 4, Legislative and Strategic Drivers, has been removed.
- The processes originally found in Sec. 5, Measures Development Process, and Sec. 6, Information Security Measurement Implementation, have been reworked into a single process and can now be found in Sec. 3, Implementation an Information Security Measurement Program.
- A new Sec. 1.4, Document Terminology, explores terminology that is relevant to the measurement and analysis of information security.
- A new Sec. 2, Fundamentals, explores measurement program benefits, program scope, foundations for a successful program, roles and responsibilities, the programmatic value of metrics, measures communication, organizational considerations, manageability, and data management concerns.
- Section 3.5, Information Security Measurement Program, has been removed.
- The information originally found in Sec. 5.5, Measures Development and Selection, has been expanded and can be found in SP 800-55v1.
- Appendix A, Candidate Measures, was removed.