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

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

Public Comment Period
January 17, 2024 – March 18, 2024

Submit Comments
cyber-measures@list.nist.gov

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

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

Abstract

This document provides guidance on how an organization can 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.

Call for Patent Claims

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

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

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

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

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

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

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

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

Such statements should be addressed to: cyber-measures@list.nist.gov

Note to Reviewers

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

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

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

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

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 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. While "program" is used in the development and implementation of cybersecurity 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 implementation, efficiency, and effectiveness to an organization's success in its business activities. In this document, the term "controls" is used broadly to describe identified countermeasures to manage information security risks. It is intended to be framework- or standard-agnostic and can also apply to other existing models or frameworks that might be used in an organization.

Where this document provides a methodology for developing and implementing an information security measurement program, SP 800-55v1 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 Publications

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

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

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

1.3. Document Organization

The remaining sections of this document discuss the following:

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

1.4. Document Terminology

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

- **Information security:**[1] The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. [6]
- **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.
- **Qualitative assessment:** The use of a set of methods, principles, or rules for assessing risk based on non-numerical categories or levels. [2]
- **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 the context of the assessment. [2]
- **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. [2]
- **Measurement:** The process of obtaining quantitative values using quantitative methods.
- **Measures:** Quantifiable and objective values resulting from measurement.
- **Metrics:** Measures and assessment results designed to track progress, facilitate decision-making, and improve performance with respect to a set target.

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

2. Fundamentals

A comprehensive information security measurement program provides substantive justifications for 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 covers an evaluation of the existing security program, the identification and prioritization of potential measures, and an implementation 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 also assists in preparing required reports related to information security performance. For this reason, a measurement program needs support from across the organizational structure.

2.1. Measurement Program Benefits

Organizations want to know how well they are managing their information security risk, 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 measurement program can answer questions about information security risk management by providing a structure that helps organizations collect and analyze data. It can also enable 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.

Additionally, an information security measurement program can increase accountability by helping organizations identify specific controls that are implemented incorrectly, 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 organizational commitment to proactive information security and continuous improvement. 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 has 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 regarding the implementation, effectiveness, and impact of controls. This 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. A foundation of strong upper-level management support
2. Practical information security policies and procedures
3. Quantifiable measures
4. Results-oriented measures analysis

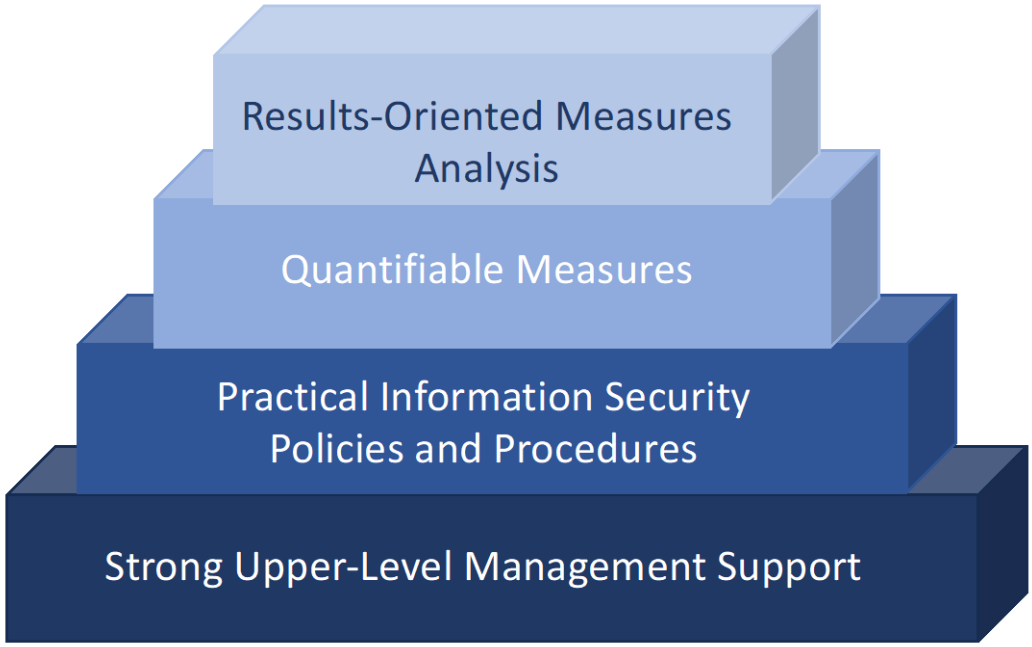


Fig. 1. Information security measurement program structure

A foundation of strong upper-level management support 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. The 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 information resources.

An effective information security measurement program also has 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 create the foundation needed to 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 be developed and established to capture and provide meaningful performance data. The goal of these measure is to be easily obtainable, feasible to measure, and repeatable, in order to show relevant performance trends, track performance, and direct resources.

Finally, the information security measurement program will emphasize consistent periodic analyses of the measures data. Lessons learned from these analyses can improve the effectiveness of existing controls and help plan the implementation of future controls. To ensure that the collected data is meaningful and useful, 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 information security is the responsibility of all organization members, 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. The functions and responsibilities listed below will be owned by someone within the organizational structure even when organizational structures vary. The application of a measurement program as described in this publication is intended to be flexible and allow organizations to manage their measurement needs.

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
- Ensuring that information security measurement activities have adequate financial and human resources for success
- Actively promoting information security measurement as an essential facilitator of information security performance improvement throughout the organization
- Approving policies to officially institute measures collection

Chief Information Officer[2]

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

- Ensuring 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 financial and human resources to the information security measurement program
- Regularly reviewing information security measures and using that data 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 address issues discovered through measures analysis and taking corrective actions, such as revising information security procedures and providing additional information security training to staff
- Issuing policies, procedures, and guidelines to officially develop, implement, and institute measures

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

Chief Information Security Officer

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

- Developing and implementing information security measures
- Integrating information security measurement into the process for planning, implementing, evaluating, and documenting remedial actions to address any 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 any internal guidelines or policies related to information security measures
- Using 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

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
- 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
- Ensuring 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 it for policy, resource allocation, and budget decisions
- Supporting the implementation of corrective actions identified through measuring information security performance

Other Roles

The information security measurement responsibilities of those 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

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

2.5. Programmatic Value of Metrics

Metrics are designed to track progress, facilitate decision-making, and improve performance by providing insight into how an organization is performing. 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.

2.6. Aggregation and Communication

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

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

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

While incredibly valuable, 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 the reporting. For example, when aggregating measures to communicate about risk the following considerations are helpful:

- What measures tell a more precise risk story?
- 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 report on in communications. More information on developing, selecting, and evaluating measures that fit the needs of an organization can be found in SP 800-55v1.

Aggregation and communication about information security measures can be small or large and 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 larger annual report will require measures related to all the topics covered in the report. The specific needs and reporting structure of a request for information will determine what data needs to be aggregated.

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, it will consider the specific organizational structure, processes, required budget, personnel, and time resources to 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 are 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.[3] 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 it, and at what intervals. Operationally, this may include identifying relevant data sources, determining granularity, and validating data accuracy. The information security measurement program also can ensure that clear metadata is used by defining how data will be normalized with consistent units and formats and ensuring accurate aggregation and meaningful comparisons. 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.

[3] 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. Information Security Measurement Program

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

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

The activities outlined in **Fig. 2** do not need to be done sequentially. 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 to develop and implement an information security measurement program. The process can be applied across different levels of the organization.

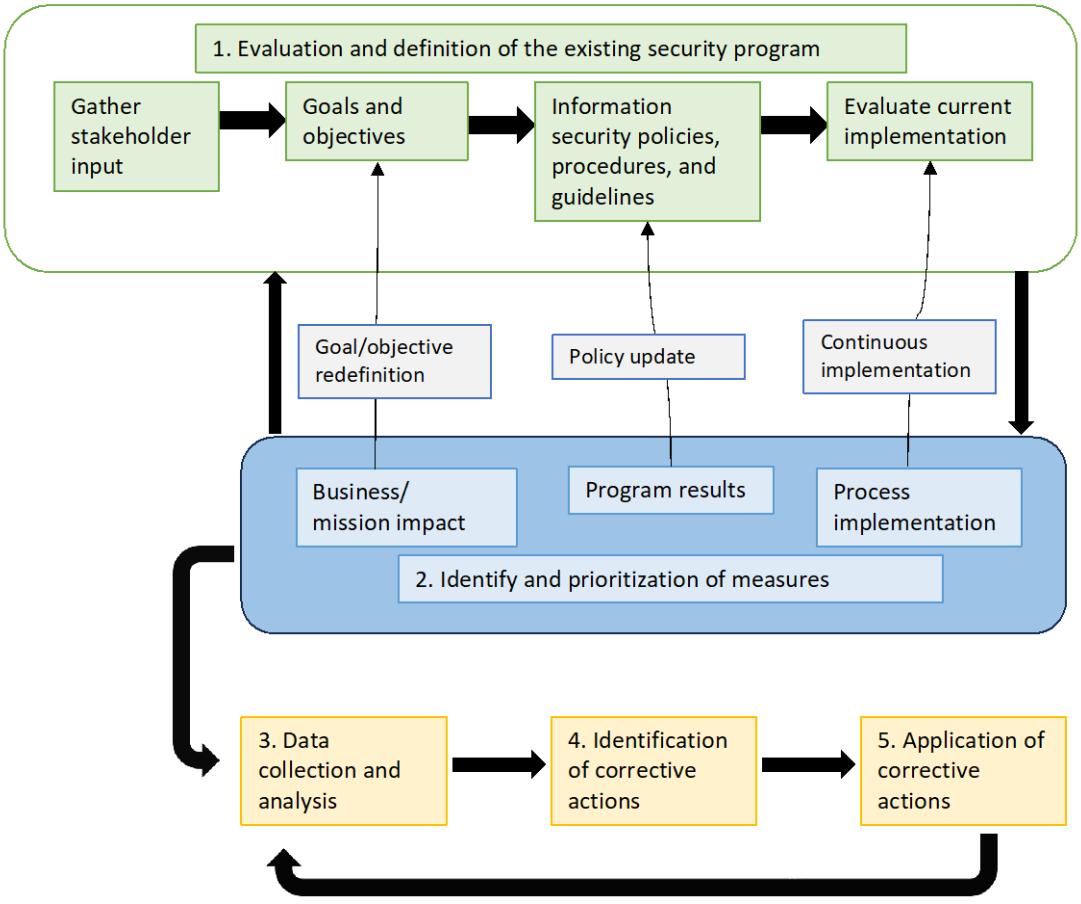


Fig. 2. Information security measurement program workflow

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

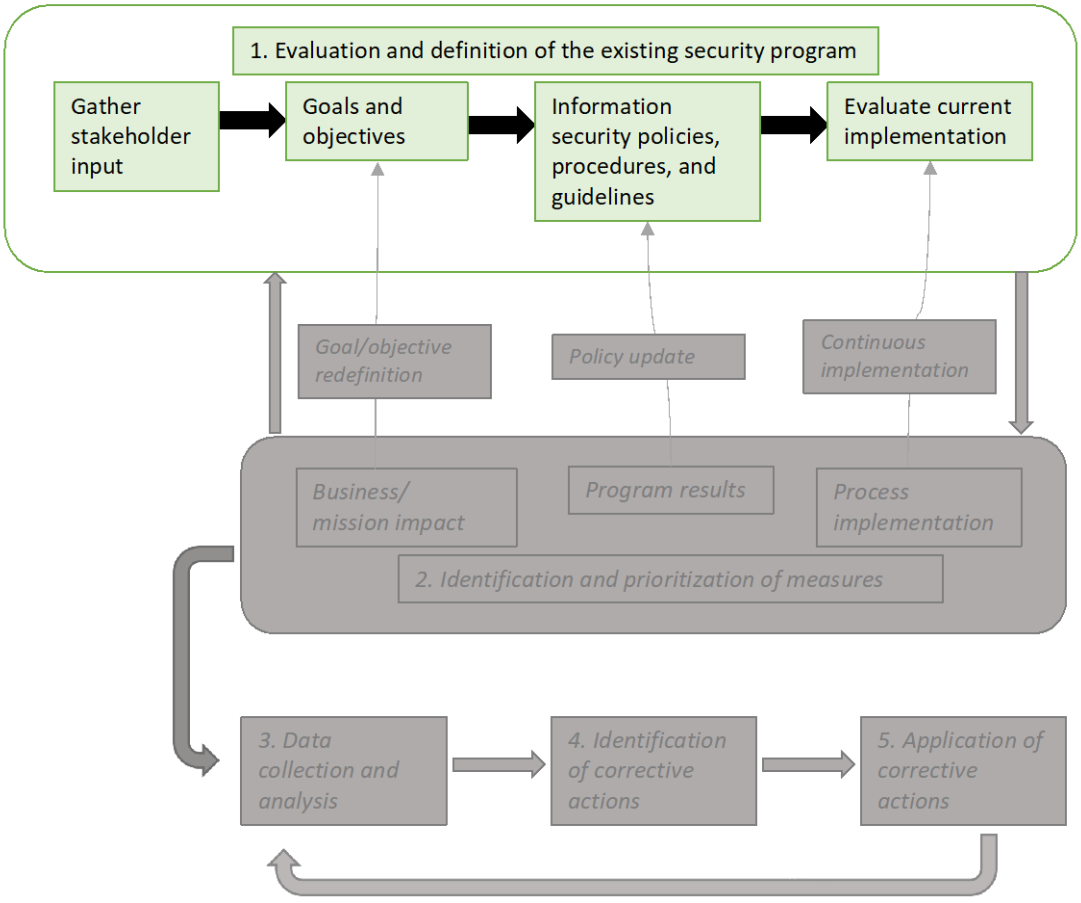


Fig. 3. Evaluation and definition of the existing security program

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 role. 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. Any organizational element responsible for measurement is also included.

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. Further information can be gathered by considering system-level measurement needs. 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. These 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 are reviewed to extract relevant information security performance goals and objectives, many of which will be identified when gathering stakeholder input. Existing metrics may also be included when identifying organizational goals and objectives. These 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.

3.1.4. Evaluating Current Implementation

Any existing measures and data repositories that are used to derive measures data are reviewed to identify appropriate implementation evidence. Implementation evidence points to aspects of controls that indicate 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 system security requirements, processes, and procedures can be extracted by consulting multiple sources, including documents, interviews, and observation.

Aggregating multiple system evaluations is essential for 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 looking at the results of regularly conducted 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.

3.2. Identify and Prioritize Measures

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

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

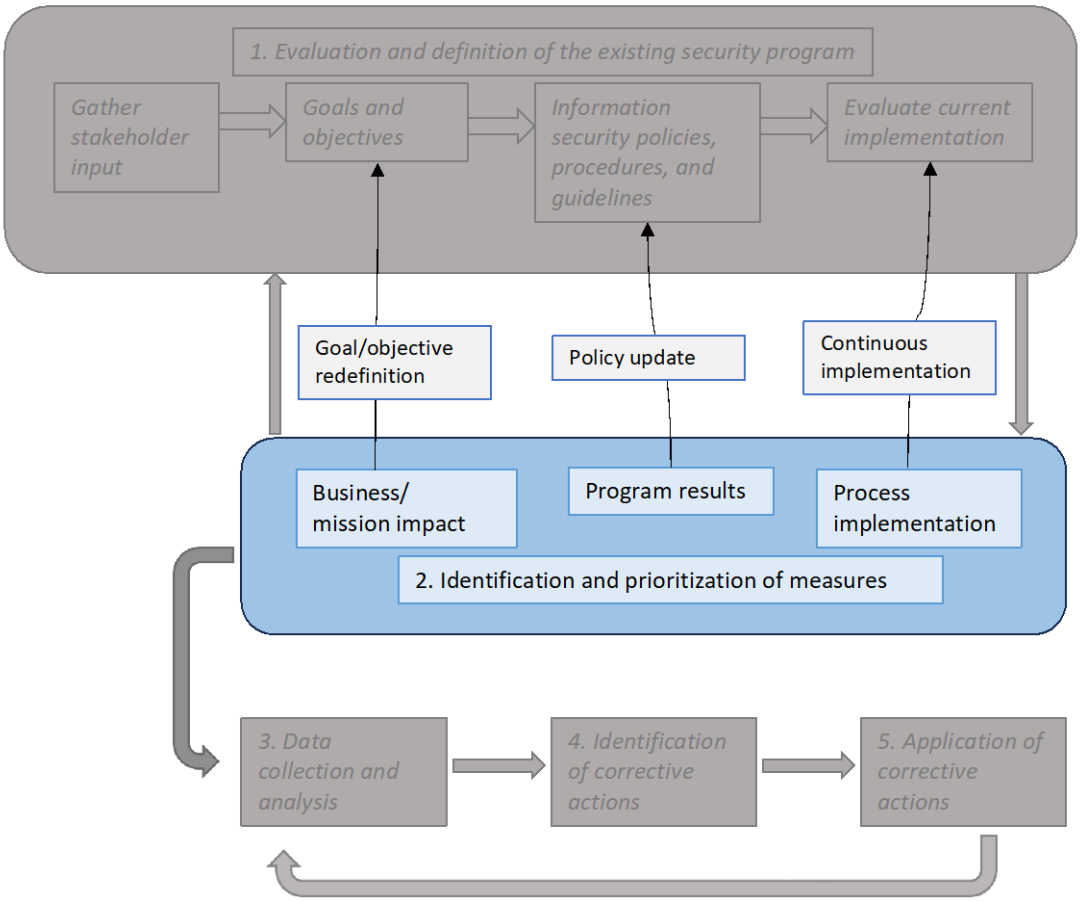


Fig. 4. Identify and prioritize measures

The existence and institutionalization of processes and procedures is 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 more standardized and repeatable, and the program can produce a greater quantity and quality of data that can be used 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 the desired outcome. Efficiency measures monitor the speed with which processes and controls are returning 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 continues to develop.

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.[5] 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.

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

[5] 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].

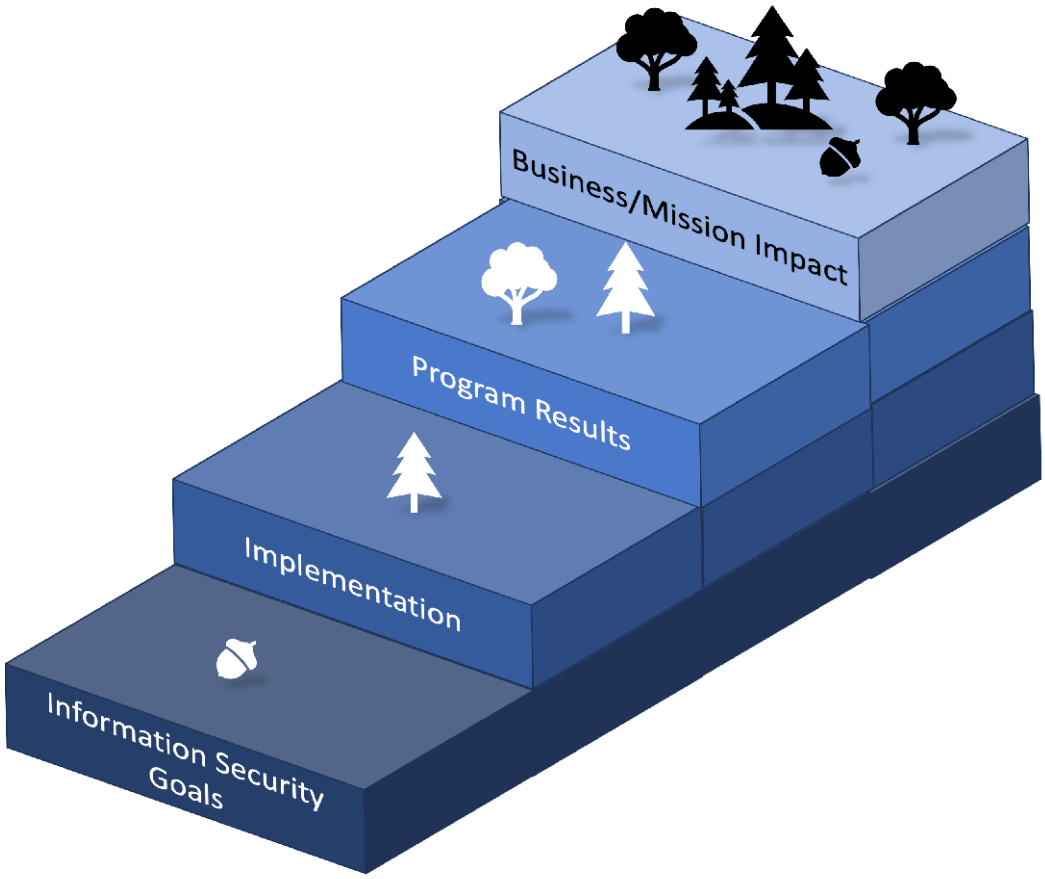
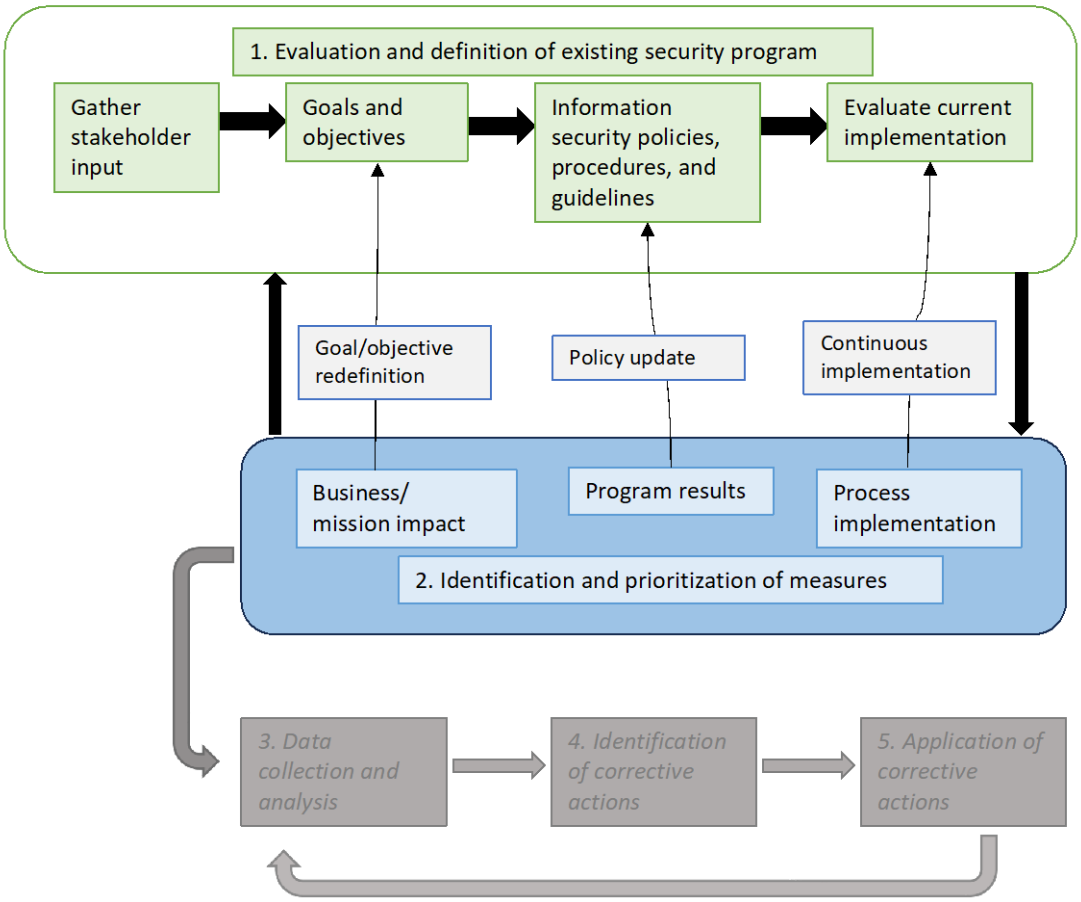


Fig. 5. Information security program development and types of measurement

Measures that are ultimately selected for implementation will be useful for measuring performance, identifying causes of unsatisfactory performance, pinpointing improvement areas, facilitating consistent policy implementation, effecting security policy changes, redefining goals and objectives, and supporting 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.



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**.

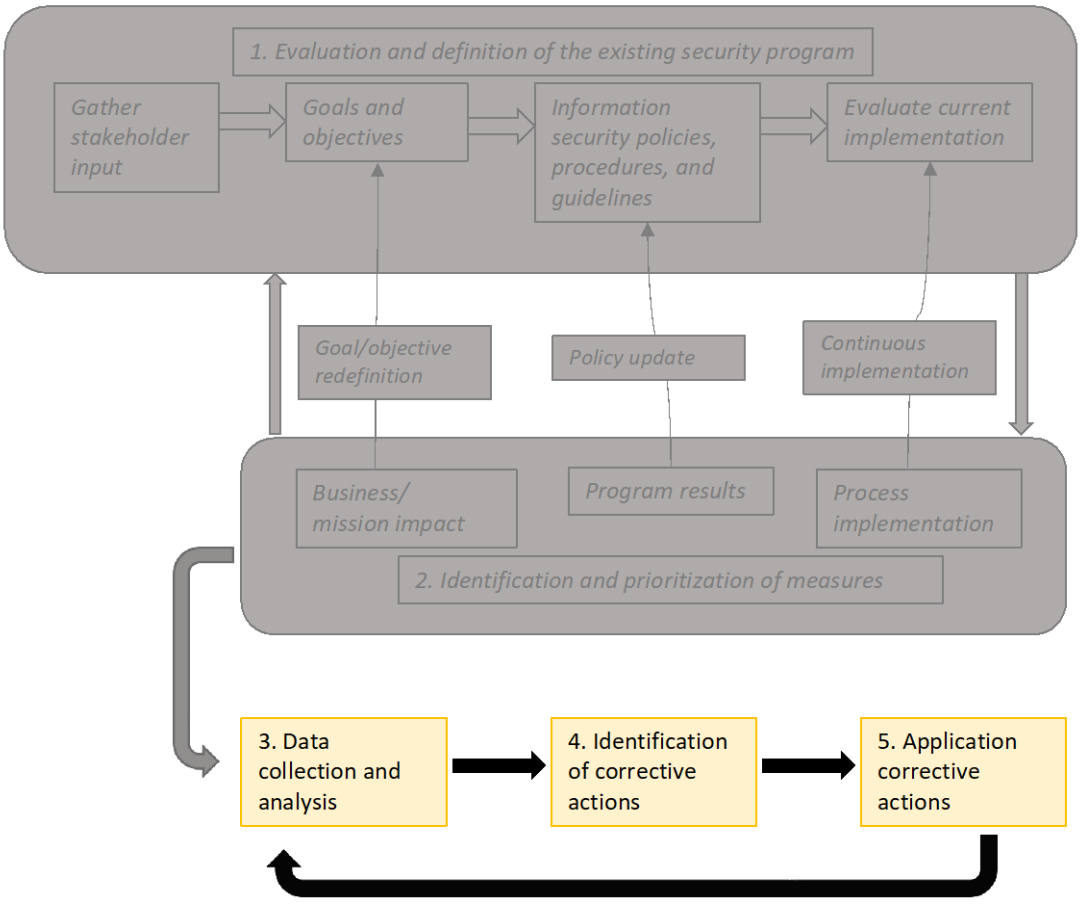


Fig. 7. Information security measurement implementation

3.3.1. Identify and Prioritize Measures

Data collection and analysis involve activities that are essential for ensuring that collected measures are used to understand the organization's information security posture and identify 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 it in a format 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.

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.

3.3.2. 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.

> Moving from identifying corrective actions to *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.

3.3.3. Apply Corrective Actions

Applying corrective actions involves implementing corrective actions 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.[6]

Iterative data collection, analysis, and reporting will track the progress of corrective actions, measure improvement, and identify areas where further improvement is needed. The nature of the cycle monitors progress and ensures that corrective actions are influencing 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.

[6] 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) 800-137A. https://doi.org/10.6028/NIST.SP.800-137A

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

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

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

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

[6] 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

[7] 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

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

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. [6]

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 non-numerical categories or levels. [7]

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. [7]

Appendix B. Change Log

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

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

- …