Field	Data
Measure ID	Security Training Measure 1
Goal	Strategic Goal: Ensure a high-quality workforce supported by modern and secure infrastructure and operational capabilities. Information Security Goal: Ensure that organization personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
Measure	Percentage (%) of information security personnel that have received security training. NIST SP 800-53 controls: AT-3: Security Training
Measure Type	Implementation
Formula	(Number of information security personnel that have completed security training within the past year divided by the total number of information security personnel) multiplied by 100
Target	This should be a high percentage defined by the organization. (E.g. 100%)
Implementation Evidence	1. Are significant security responsibilities defined with qualifications criteria and documented in policy (AT-1 and PS-2)? Yes/No 2. Are records kept regarding which employees have significant security responsibilities (AT-3)? Yes/No. 3. How many employees in your department have significant security responsibilities (AT-3)? ________ 4. Are training records maintained (AT-4)? (Training records indicate the training that specific employees have received.) Yes/No

Table 7-2 Example performance measures documentation

Field	Data
	5. How many of those with significant security responsibilities have received the required training (AT-4)? ____________________ 6. If all personnel have not received training, state, all reasons that apply (AT-4): a. Insufficient funding. b. Insufficient time. c. Courses unavailable. d. Employee has not registered. e. Other (specify) ____________________
Frequency	Collection Frequency: Organization-defined (example: quarterly) Reporting Frequency: Organization-defined (example: annually)
Responsible Parties	Information owner: organization-defined (example: training manager) Information collector: organization-defined (example: information security officer [ISO], training manager) Information customer: chief information officer (CIO), information security officer (ISO) (e.g., chief information security officer (CISO))
Data Source	Training and awareness tracking records
Reporting Format	Pie chart illustrating the percentage of security personnel that have received training versus those who have not received training. If performance is below target, pie chart illustrating causes of performance falling short of targets

Table 7-2 Example performance measures documentation (continued)

Source: NIST SP 800-55, Rev 1

Instructions for the development and format of this template are provided in Table 7-3.

Field	Data
Measure ID	State the unique identifier used for measure tracking and sorting. The unique identifier can be from an organization-specific naming convention or can directly reference another source.
Goal	Statement of strategic goal and/or information security goal. For system-level security control measures, the goal would guide security control implementation for that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the account was that of the selected strategic goal.
Measure	Statement of measurement. Use a numeric statement that begins with the word *percentage, number, frequency, average*, or a similar term. If applicable, list the NIST SP 800-53 security control(s) being measured. Security controls that provide supporting data should be stated in ample meditation evidence. If the measure is applicable to a specific FIPS 199 impact level (high, moderate, or low), status level within the measure.
Type	Statement of whether the measure is implementation, effectiveness/efficiency, or impact.
Formula	Calculation to be performed that results in a numeric expression of a measure. The information gathered through listing implementation evidence serves as an input into the formula for calculating the measure.

Table 7-3 Measures template and instructions

Field	Data
Target	Threshold for a satisfactory rating for the measure, such as milestone completion or a statistical measure. Target can be expressed in percentages, time, dollars, or other appropriate units of measure. Target may be tied to a required completion timeframe. Select final and interim target to enable tracking of progress toward stated goal.
Implementation Evidence	Implementation evidence is used to compute the measure, validate that the activity is performed, and identify probable causes of unsatisfactory results for a specific measure. 1. For manual data collection, identified questions and data elements that would provide the data inputs necessary to calculate the measure's formula, qualify the measure for acceptance, and validate provided information 2. For each question or query, status security control number from NIST SP 800-53 that provides information, if applicable 3. If the measure is applicable to a specific FIPS 199 impact level, questions should state the impact level 4. For automated data collection, identified data elements that would be required for the formula, qualify the measure for acceptance, and validate the information provided
Frequency	Indication of how often the data is collected and analyzed, and how often the data is reported. State the frequency of data collection based on a rate of change in a particular security control that is being evaluated. State the frequency of data reporting based on external reporting requirements and internal customer preferences.
Responsible Parties	Indicate the following key stakeholders: • Information owner: Identify organizational component, an individual who owns required pieces of information • Information collector: Identify the organizational component and individual responsible for collecting the data: (Note: if possible, information collector should be a different individual or even a representative of a different organizational unit than the information owner, to avoid the possibility of conflict of interest and ensure separation of duties. Smaller organizations will need to determine whether it is feasible to separate these two responsibilities.) • Information customer: Identify the organizational component and individual who will receive the data.
Data Source	Location of the data to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.
Reporting Format	Indication of how the measure will be reported, such as pie charts, line charts, bar graphs, or other format. State the type of format or provide a sample.

Table 7-3 Measures template and instructions (continued)

Source: NIST SP 800-55, Rev 1

Candidate Measures A number of example candidate measures are provided in Table 7-4. Additional details on these measures, including how they are calculated and used, are provided in SP 800-55, Rev 1.

Information Security Performance Measurement Implementation

Once developed, information security performance measures must be implemented and integrated into ongoing information security management operations. For the most part, it is insufficient to simply collect these measures once (although some activities only require the collection of data for one particular purpose, such as certification and accreditation, described later in this chapter). Performance measurement is an ongoing, continuous improvement operation.