THEME 5

Systems of informational security

Telecommunication systems department

Lecturer: assistant professor Persikov Anatoliy Valentinovich

PERFORMANCE MEASURES

A performance measures program provides numerous organizational and financial benefits to federal agencies. Agencies can develop information security metrics that measure the effectiveness of their security program, and provide data to be analyzed and used by program managers and system owners to isolate problems, justify investment requests, and target funds specifically to the areas in need of improvement. By using metrics to target security investments, agencies can get the best value from available resources. The typical information performance management program consists of four interdependent components: senior management support, security policies and procedures, quantifiable performance metrics, and analyses.

Strong senior management support establishes a focus on security within the highest levels of the organization. Without a solid foundation (e.g., proactive support of those persons in positions that control information resources), the effectiveness of the security metrics program can fail when pressured by politics and budget limitations. The second component of an effective security metrics program is practical security policies and procedures backed by the authority necessary to enforce compliance. Metrics are not easily obtainable in the absence of policies and procedures. The third component is developing and establishing quantifiable performance metrics that are designed to capture and provide meaningful performance data.

PERFORMANCE MEASURES

To provide meaningful data, quantifiable security metrics must be based on information security performance goals and objectives, and be easily obtainable, repeatable, relevant, useful, and measurable. Finally, the security metrics program itself must emphasize consistent, periodic analysis of the metrics data. The results of this analysis are used to apply lessons learned, improve the effectiveness of existing security controls, and plan future controls to meet new security requirements as they occur. Accurate data collection must be a priority with stakeholders and users if the collected data is to be meaningful to the management and improvement of the overall security program.

A number of existing laws, rules, and regulations cite information technology (IT) performance measurement in general and information security performance measurement in particular, as requirements. These laws include the Clinger-Cohen Act, Government Performance and Results Act (GPRA), Government Paperwork Elimination Act (GPEA), and the Federal Information Security Management Act (FISMA).

PERFORMANCE MEASURES

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55, **Security Metrics Guide for Information Technology Systems**, provides guidance on how an organization, by using metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or how to identify and evaluate nonproductive controls. It explains the metrics development and implementation process and how it can also be used to adequately justify security control investments. The results of an effective metrics program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports.

Fiscal constraints and market conditions compel government and industry to operate on reduced budgets. In such an environment, it is difficult to justify broad investments in the information security infrastructure. Historically, arguments for investing in specific areas of information security lack detail and specificity and fail to adequately mitigate specific system risk. Information security metrics can facilitate the **capital planning and investment control** (CPIC) process by providing quantifiable information for business case development. Information security metrics can also assist with determining the effectiveness of implemented information security processes, procedures, and controls by relating results of information security activities (e.g., incident data, revenue lost to cyber attacks) to the respective requirements and to information security investments.

METRIC TYPES

Metrics are tools that support decision making. Like experience, external mandates, and strategies, metrics are one element of a manager's toolkit for making and substantiating decisions.

Metrics are used to answer three basic questions:

- "Am I implementing the tasks for which I am responsible?" Consider the example of a program manager with responsibility for 250 information systems. Among other things, that manager is responsible for the security certification and accreditation of those systems. A commonly used implementation metric for security certification and accreditation is the percentage of systems accredited.

METRIC TYPES

- "How efficiently or effectively am I accomplishing those tasks?" Such metrics often answer more complex questions after an activity is fully implemented. For example, federal law requires that security certification and accreditation take place following a major system change. One might measure the efficiency of a security certification and accreditation program by determining the time lag between each major system change and that system's renewed accreditation. Or one might measure the effectiveness of a security certification and accreditation program by determining the number of accredited systems whose certification process included the creation of a system security plan.

- "What impact are those tasks having on the mission?" Activities are initially selected with the belief that they will contribute to the mission. After an activity is shown to be fully implemented, managers must validate that the activity is delivering the expected benefit. These metrics are the most difficult to generate. A security certification and accreditation process may prove to have an impact by showing that fewer interruptions or losses of data due to security incidents are experienced among correctly accredited systems than among incorrectly accredited or nonaccredited systems.

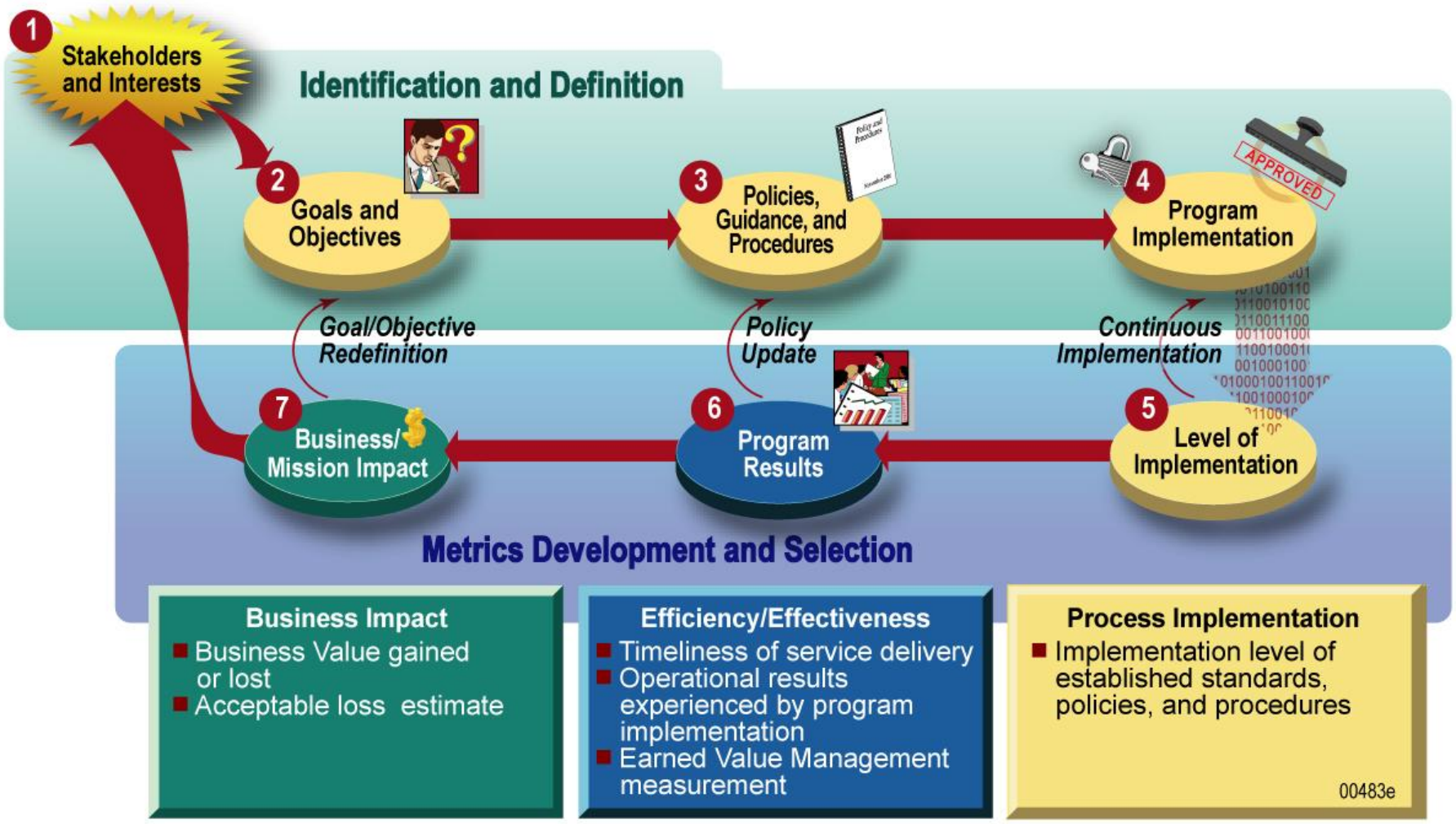
METRICS DEVELOPMENT AND IMPLEMENTATION APPROACH

Two processes guide the establishment and operation of an information security metrics program: metrics development and metrics implementation.

The metrics development process establishes the initial set of metrics and selection of the metrics subset appropriate for an organization at a given time.

The metrics program implementation process operates a metrics program that is iterative by nature and ensures that appropriate aspects of information security are measured for a specific time period.

METRICS DEVELOPMENT PROCESS



METRICS DEVELOPMENT PROCESS

The information security metrics development process consists of two major activities:

1) Identifying and defining the current information security program; and
2) Developing and selecting specific metrics to measure implementation, efficiency, effectiveness, and the impact of the security controls.

The process steps do not need to be sequential. Rather the process provides a framework for thinking about metrics and aids in identifying metrics to be developed for each system. The type of metric depends on where the system is within its life cycle and on the maturity of the information system security program. This framework facilitates tailoring metrics to a specific organization and to the different stakeholder groups present within each organization.

METRICS DEVELOPMENT PROCESS

Phases 5, 6, and 7 involve developing metrics that measure process implementation, effectiveness and efficiency, and mission impact. The specific aspect of information security that metrics will focus on at any given point will depend on information security program maturity. Implementation evidence, required to prove higher levels of effectiveness, will change from establishing existence of policy and procedures to quantifying implementation of these policies and procedures, then to quantifying results of implementation of policies and procedures, and ultimately to identifying the impact of implementation on the organization's mission.

METRICS DEVELOPMENT PROCESS

Based on existing policies and procedures, the universe of possible metrics can be prohibitively large; therefore, agencies should prioritize metrics to ensure that the final set selected for initial implementation has the following attributes:

- Facilitates improvement of high-priority security control implementation. High priority may be defined by the latest GAO or IG reports, results of a risk assessment, or an internal organizational goal;
- Uses data that can realistically be obtained from existing processes and data repositories; and
- Measures processes that already exist and are relatively stable. Measuring nonexistent or unstable processes will not provide meaningful information about security performance and will therefore not be useful for targeting specific aspects of performance. On the other hand, attempting such measurement may not be entirely useless, because such a metric will certainly produce poor results and will therefore identify an area that needs improvement.

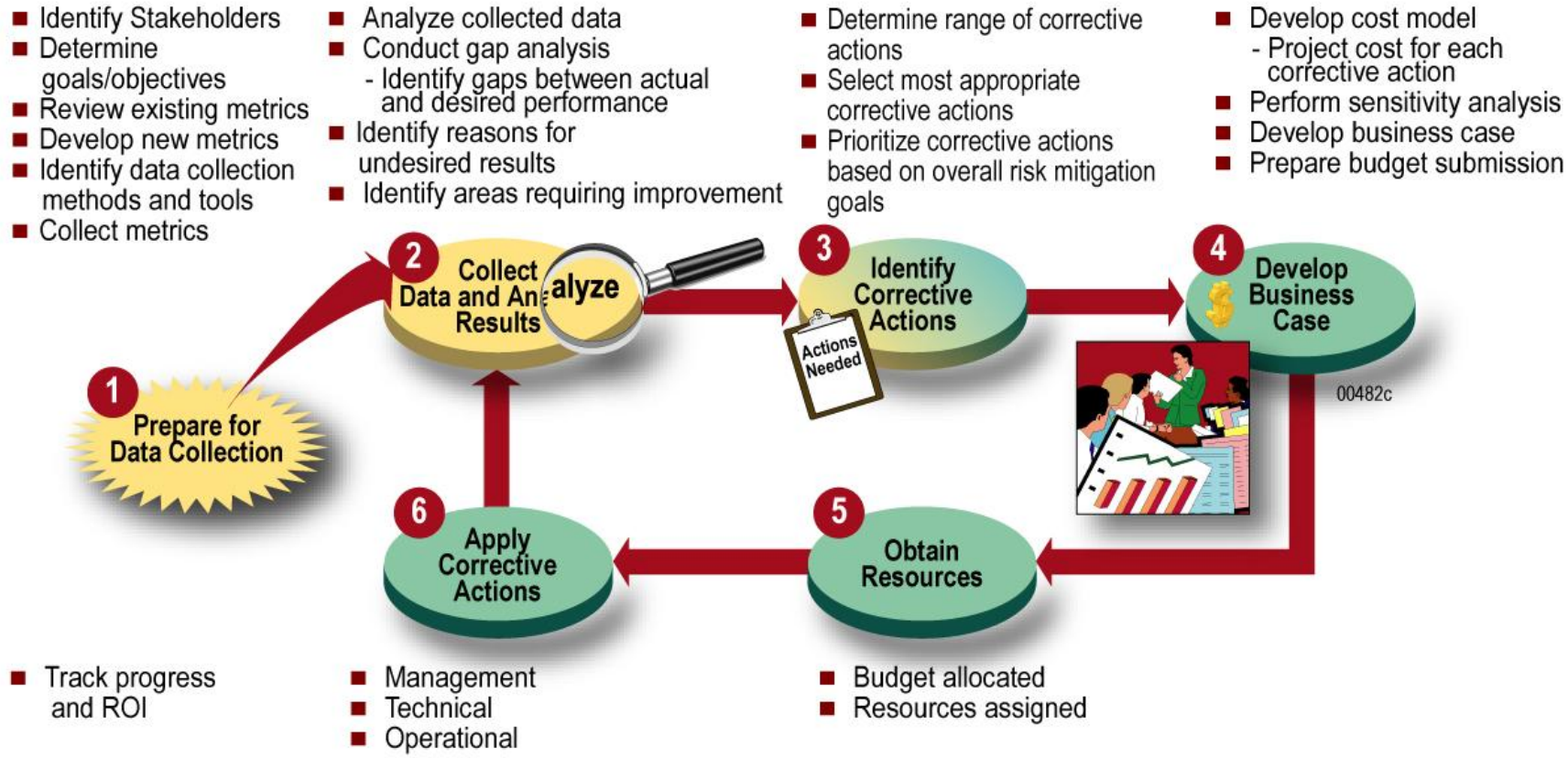
METRICS DEVELOPMENT PROCESS

Metrics can be derived from existing data sources, including security certification and accreditation, security assessments, plan of action and milestones (POA&M), incident statistics, and agency-initiated or independent reviews. Agencies may decide to use a weighting scale to differentiate the importance of selected metrics and to ensure that the results accurately reflect existing security program priorities. This process would involve assigning values to each metric based on the importance of a metric in the context of the overall security program. Metrics weighting should be based on the overall risk mitigation goals, is likely to reflect higher criticality of department-level initiatives versus smaller-scale initiatives, and is a useful tool that facilitates integration of information security into the departmental capital planning process.

A phased approach may be required to identify short-, mid-, and long-term metrics in which the implementation time frame depends on a combination of system-level effectiveness, metric priority, data availability, and process stability. Once applicable metrics that contain the qualities described above are identified, they will need to be documented with supporting detail, including frequency of data collection, data source, formula for calculation, implementation evidence for measured activity, and a guide for metric data interpretation. Other information about each metric can be defined based on an organization's processing and business requirements.

METRICS PROGRAM IMPLEMENTATION

Information security metrics should be used for monitoring information security control performance and initiating performance improvement actions. This iterative process consists of six phases.



PREPARE FOR DATA COLLECTION

Phase 1 of the process, Prepare for Data Collection, involves activities that are key for establishing a comprehensive information security metrics program. These activities include the information security metrics identification, definition, development, and selection activities, and developing a metrics program implementation plan.

After the metrics have been identified, specific implementation steps should be defined on how to collect, analyze, and report the metrics. These steps should be documented in the metrics program implementation plan.

PREPARE FOR DATA COLLECTION

The following items may be included in the plan:

- Metrics roles and responsibilities, including responsibilities for data collection (both soliciting and submitting), analysis, and reporting;
- An audience for the plan;
- Process of metrics collection, analysis, and reporting that is tailored to the specific organizational structure, processes, policies, and procedures;
- Details of coordination with the chief information officer (CIO), such as with risk assessment, security certification and accreditation, and FISMA reporting activities;
- Details of coordination between the CIO and other functions within the agency, external to the CIO (e.g., Information Assurance (IA), if separate from the CIO; physical security; personnel security; and critical infrastructure protection [CIP]) to ensure that the metrics data collection is streamlined and nonintrusive;
- Creation or selection of data collection and tracking tools;
- Modifications of data collection and tracking tools; and
- Metrics summary reporting formats.

THANKS FOR ATTENTION