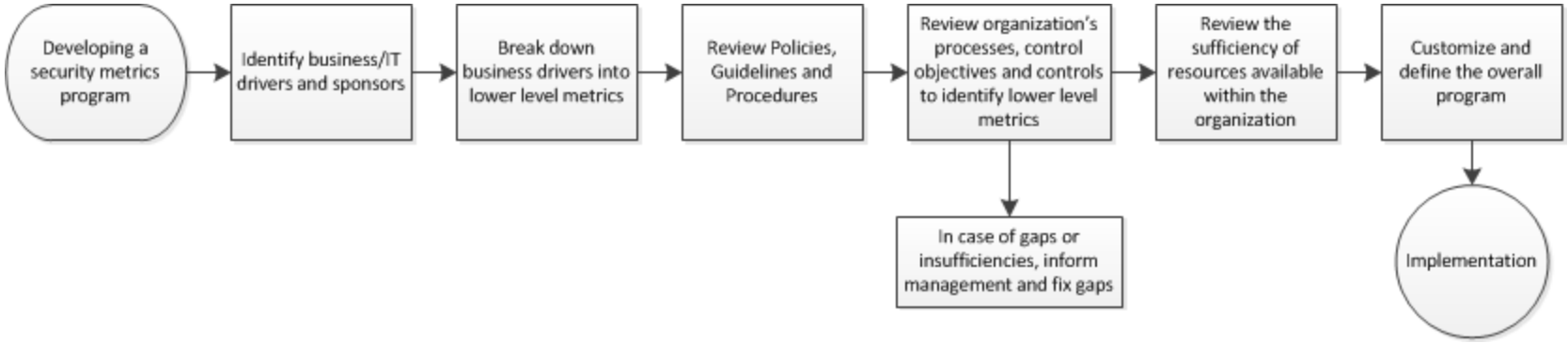
# HANDOUT A:
# DESIGNING, IMPLEMENTING AND SUSTAINING A METRICS PROGRAM

ISACA®
Trust in, and value from, information systems
San Francisco Chapter


2013 Fall Conference – "Sail to Success"

# Handout A: Developing a Security metrics program




- Identify business/IT drivers for the program and sponsors
- Break down business drivers to ensure lower level metrics are derived from higher level requirements (top-down iteration). In most cases, this shall include benchmarks / targets.
- Review Policies, Guidelines and Procedures to identify leverage points
- Review organization's processes, control objectives and controls to determine how to address lower level metrics requirements with existing framework
- In case of gaps or insufficiencies, inform management and fix gaps
- Review the sufficiency of resources (processes, evidence, human resources) available within the organization to meet program requirements (bottom-to-top iteration)
- Customize the model for overall program by documenting the program structure, the metrics to be collected, metrics hierarchy, data attributes, data collection specifications, data analysis and reporting procedures, visualization, presentation and reporting specifications, etc.

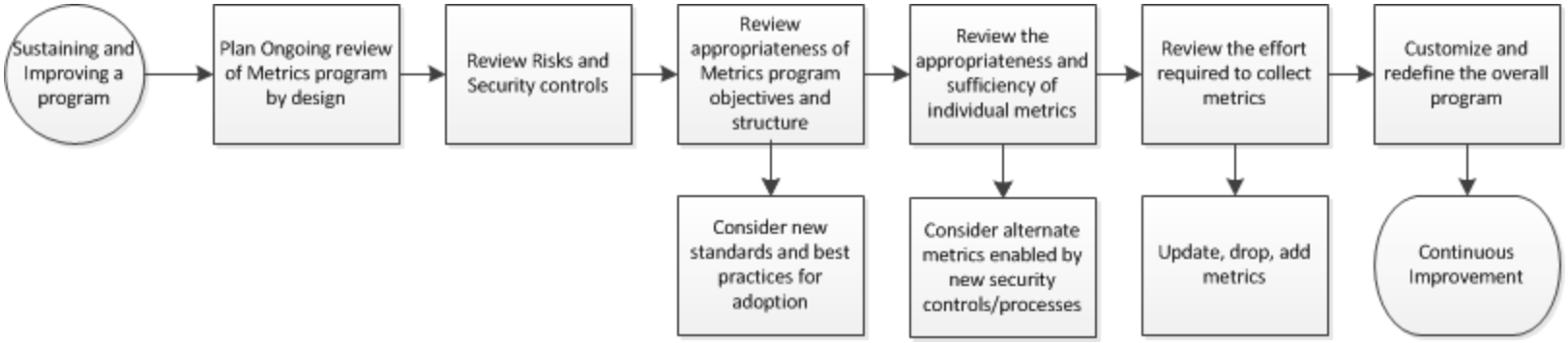
# Handout A: Implementing a security metrics program


- Start small
  - Prioritize and start with a small number of processes
  - focus on one or two key metrics that would indicate the performance of the process for a desired characteristic
  - Define program specs and get approvals (ex., data collected, sources, collection methods, frequency, metrics formulae, data analysis and metrics computation algorithms, reporting templates, frequency, roles and resp., etc.)
- Start focusing on essentials before expanding the scope
  - Implementation vs. Effectiveness (Ref. NIST 800-55), for example, Coverage on all systems vs. effectiveness of a control on the covered systems
- Data collection in accordance with pre-defined specs
  - Considerations for historical data vs. new data. Historical data may involve extensive work but may provide past trends. New data may require wait times before results are seen.
  - Accuracy and completeness to meet the specs defined
  - Frequency – more vs. less. Frequency of data collection, analysis and reporting and associated costs (technical, human, etc.)
  - Delegation of metrics collection, analysis and reporting tasks,
  - Training for personnel

# Handout A: Implementing a security metrics program, contd.

- Data analysis in accordance with pre-defined specs
  - Data consolidation,
  - Data and Analytical Integrity
  - Analysis to derive the metrics (results )
- Identification of gaps
  - Identification of gaps in control(s) performance
  - Root cause analysis
  - Plan for Corrective actions
  - Prioritization based on effort to implement, impact, and contribution to the overall goal
- Presentation and Reporting
  - Standardize the visualization and presentation format and reporting techniques
  - Present gaps and corrective actions
  - Audience vis-à-vis the frequency of reporting
  - Audience bias
- Remediation
  - Provide business case and obtain management approval
  - Implement separate work streams for remediation
  - Track progress through successive iterations of metrics program

# Handout A: Sustaining and Improving a security metrics program




- Make ongoing review of the entire metrics program an integral part of the program design
- Perform review as part of ongoing enterprise risk assessments or technology refresh cycle
- Review the appropriateness and sufficiency of individual metrics, taking into consideration new risk and performance indicators presented by new tools and data types (for ex., drop any metric that are of no further use for management)
- Review the current effort required to collect metrics and update as needed.
- Review emerging IT technologies, updated risks, security controls and their impact on the metrics program objectives
- Review program structure  and program definition based on new standards and best practices
- Customize and redefine the overall program in line with continuous improvement goals

# HANDOUT B:
# POPULAR METRICS PROGRAM MODELS

# Handout B: Popular models

- Center for Internet Security (CIS) Consensus Metrics
- NIST
- ISO 27004
- Other resources

# Handout B: CIS Consensus Metrics


Critical 'business' functions identified by CIS, with sample metrics and illustrative data sets provided

- **Five steps to building a program:**
  1. Select metrics ("start small")
  2. Create Data sets (includes detailed guidelines for data collection and automated processing)
  3. Implement Metrics
  4. Present results
  5. Grow the program
- **Categorizes Metrics into**
  - Management Metrics (targeted at Business Mgt.): Provide information on the performance of business functions, and the impact on the organization.
  - Operational Metrics (targeted at Security Mgt.): Used to understand and optimize the activities of business functions.
  - Technical Metrics (targeted at Security Operations): Provide technical details as well as a foundation for other metrics.
- **Metrics Scorecard covers Impact, Financial Metrics, Performance by Scope and Outcome**

# Handout B: NIST 800-55

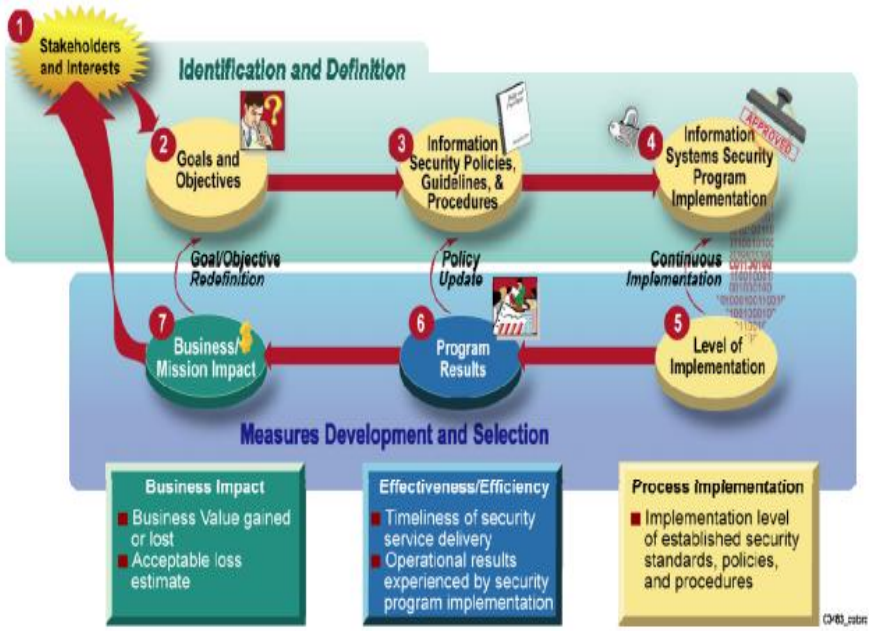



Figure 5-1. Information Security Measures Development Process

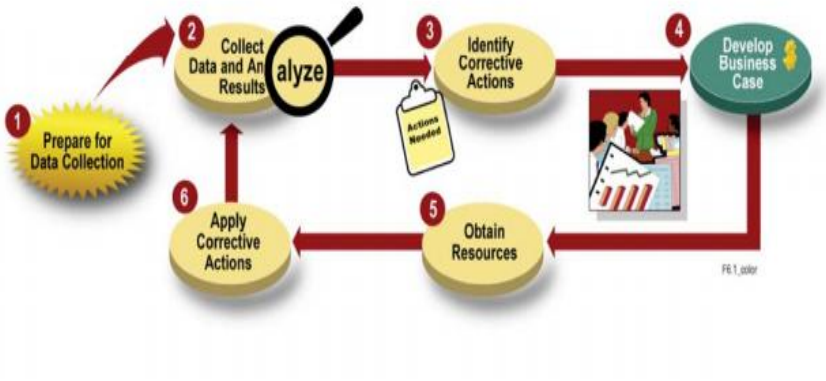
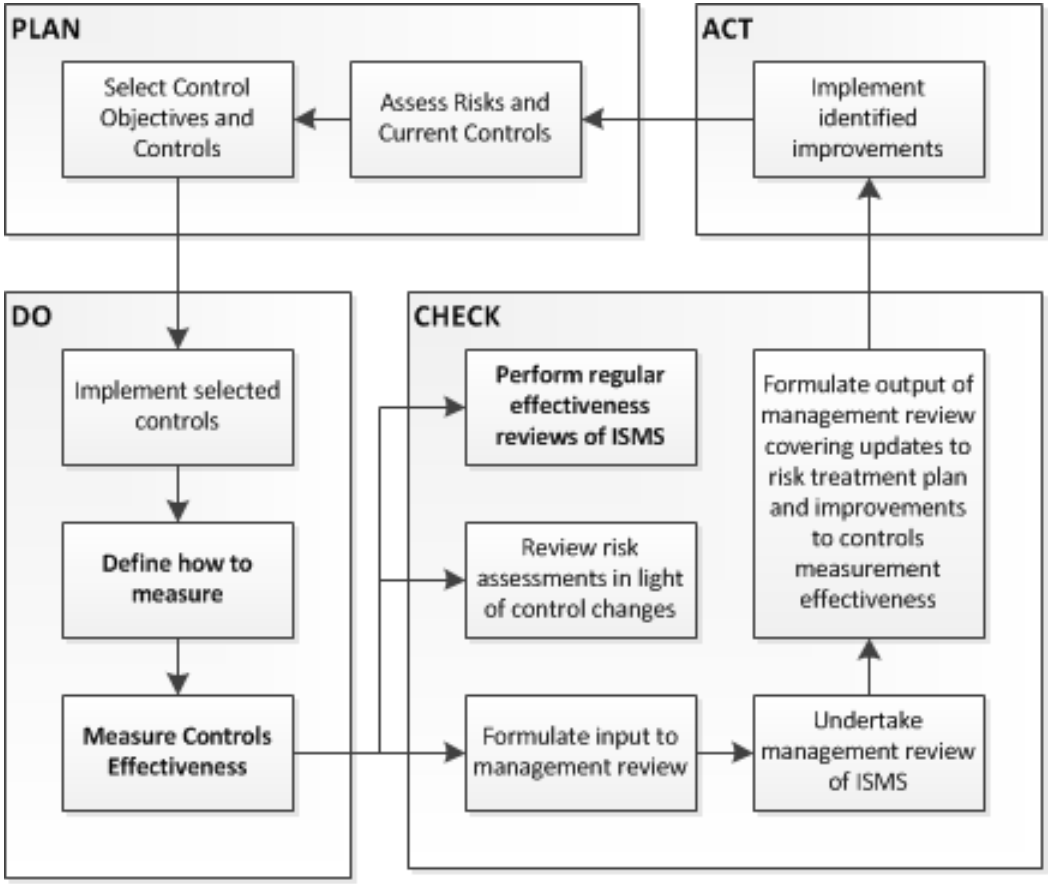



Figure 6-1. Information Security Measurement Program Implementation Process

- **Information security measures are based on information security performance goals and objectives**
- Drivers: Legislative considerations (GPRA, FISMA), Federal Enterprise Architecture, Enterprise Strategy/Planning
- Approach: Measures Development and Implementation Processes that help quantify the implementation, efficiency, and effectiveness of security controls, analyze the adequacy of information security program activities, and identify possible improvement actions

# Handout B: ISO 27004




Measurement Inputs and Outputs in ISMS PDCA Cycle of Information Security Management (summarized)

- **Four step approach**
  - Measures and Measurement Development
  - Measurement Operation
  - Data Analysis and Measurement Results Reporting
  - ISMP Evaluation and Improvement
- **Integration with other ISO standards**
- **Specifications cover base metrics, derived metrics and indicators**

# Handout B: Other resources

- Measurement of Technical Security and Program Effectiveness (A Jacquith, 2007)
  - Technical security: Perimeter defenses, Coverage and Control, Availability and reliability, Application risks, Qualitative metrics and indices
  - Program effectiveness: Planning and organization (including IT Risks, HR, Investments), Acquisition and Implementation, Delivery and Support, Monitoring
  - Case for automation
  - Metrics program management and Scorecards
  - Treatise on Visualization and Reporting