Secure One HHS

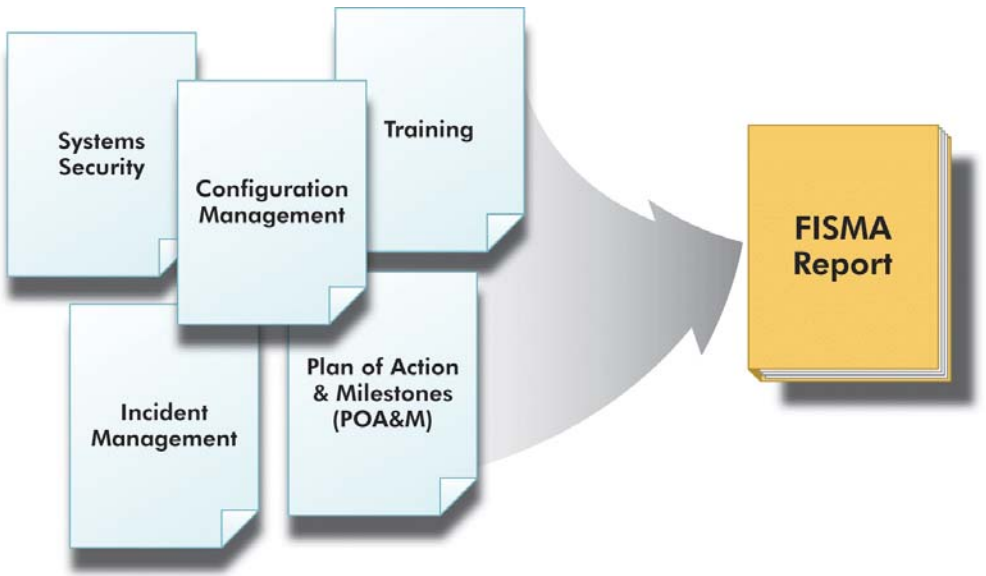
Measuring Information Security and FISMA Compliance

SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

While current FISMA metrics measure some key IT security components, they do not accurately reflect an Agency's comprehensive IT security posture

- Progress and the overall state of security should be estimated to mitigate vulnerabilities
- Resources should be devoted to standardize Inspector General evaluation methodologies
- Agencies should be required to report against performance metrics on a quarterly/annual basis to monitor progress
- Agency data should be used to populate standard dashboard templates for federal trending and distribution



SECURE ONE HHS
KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

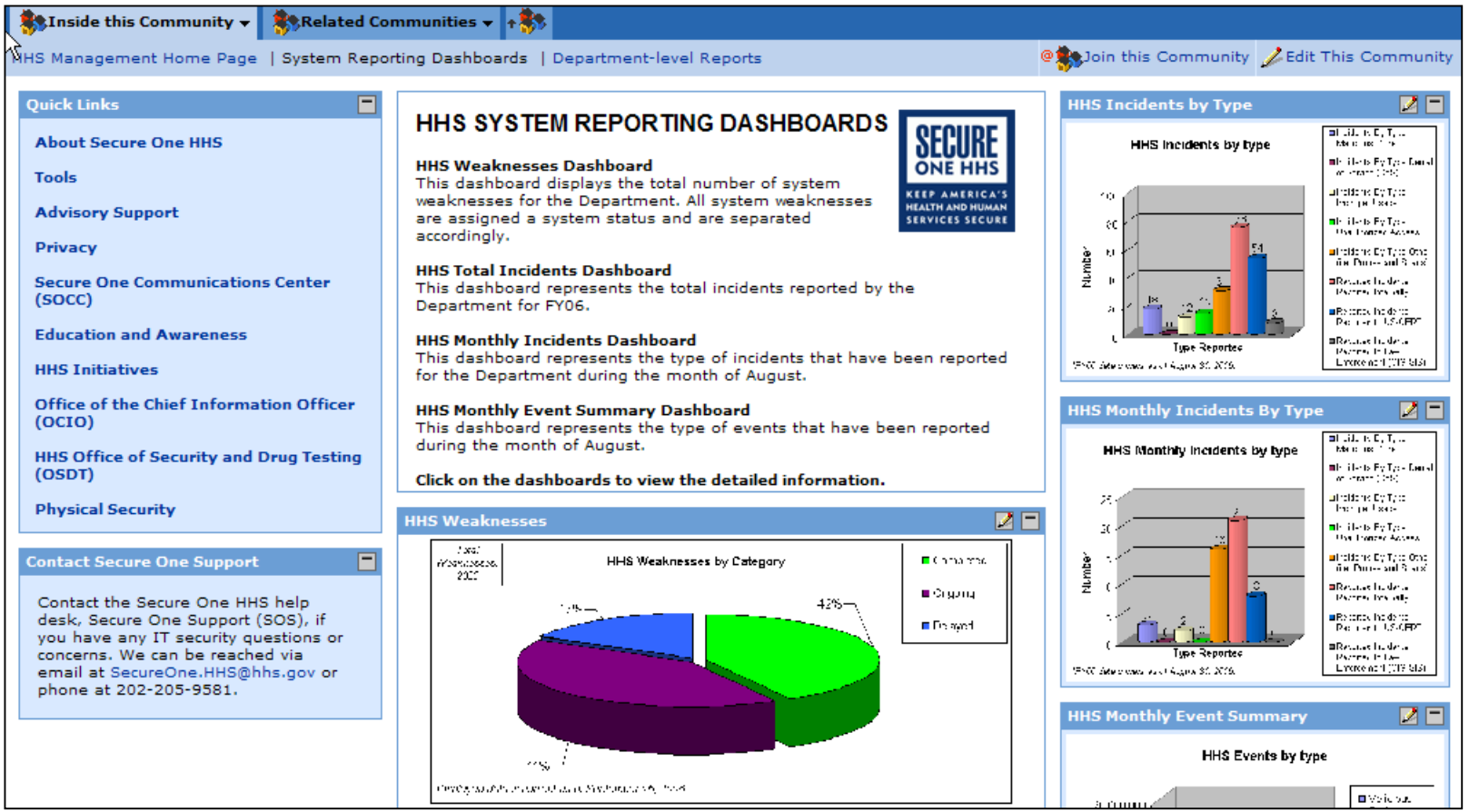
FISMA metrics must support the integration of IT security into all Agency business processes

- Provide information security protections commensurate with the risk and magnitude of potential harm
- Ensure information security management processes are integrated with agency strategic and operation planning processes
- Implement policies and procedures to cost-effectively reduce risks to an acceptable level
- Periodically test and evaluate information security controls and techniques
- Report annually on the adequacy and effectiveness of information security policies, procedures, and practices

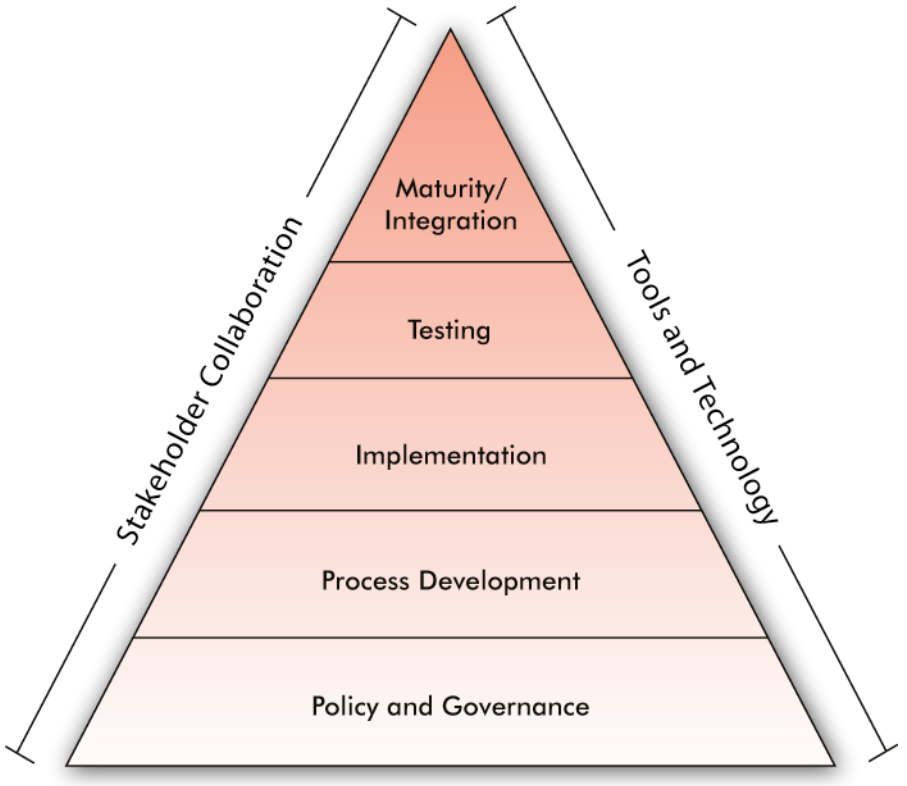
Metrics must also measure multiple facets of security program implementation

- Policy metrics – age of general information security policy, number of policies greater than three years old (older than FISMA)
  - Leading to the creation or update of policies
- Inventory metrics – age of data, frequency of update, etc.
  - Resulting in data calls and outreach, as necessary
- Process metrics – to assess the implementation of controls
  - Using NIST SP 800-53A (upon finalization) as a baseline
- Metrics on metrics – type and intent of additional metrics and/or oversight mechanisms in place
  - To determine effectiveness, necessity and compliance
- Monitoring metrics – type and frequency of network/system vulnerability scans, penetration tests, etc.
  - To formulate mitigation strategies, assign resources and ascertain real-time status reports
- Reporting metrics – timeliness, completeness and frequency of internal and external reporting, access to current and comprehensive data

HHS Metrics Dashboard Concept



Ultimately, FISMA should measure overall progress towards IT security program maturity



SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Secure One Support
Secureone.hhs@hhs.gov
202-205-9581