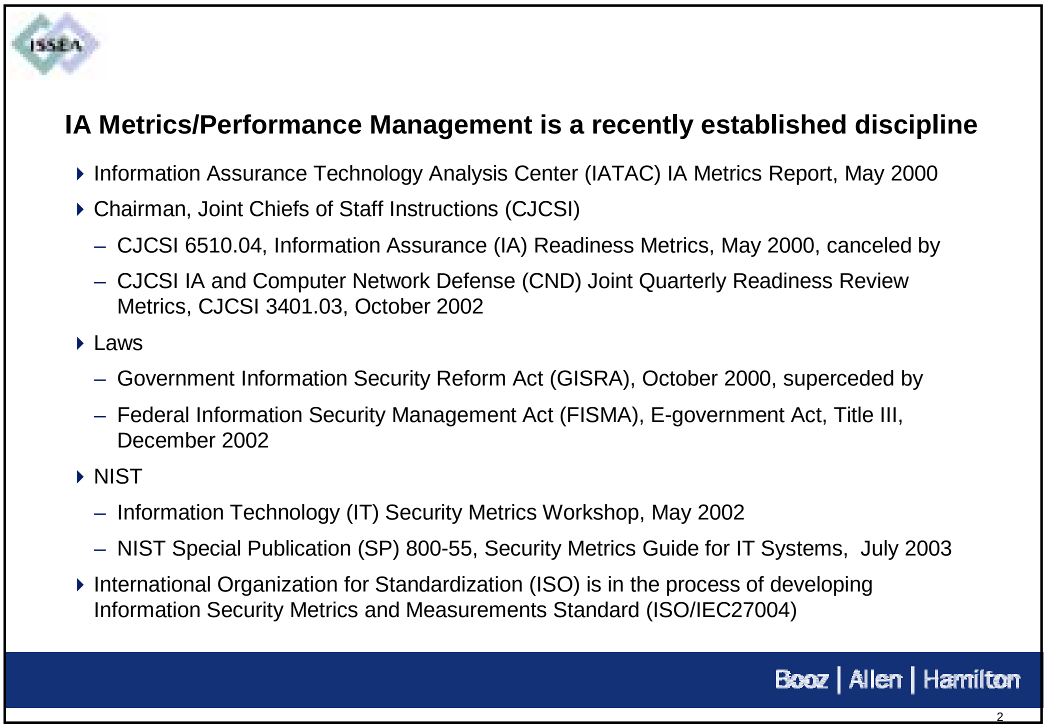
IA Metrics – Why And How To Measure Goodness Of Information Assurance

Nadya I. Bartol

PSM Users' Group Conference
July 2005

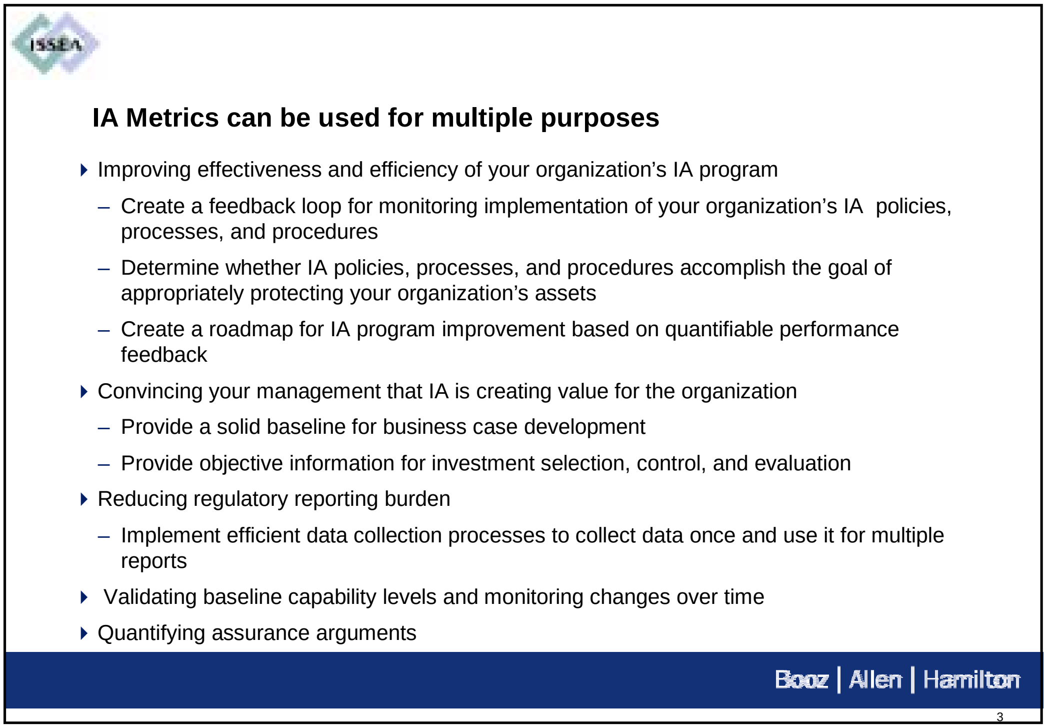
Agenda

- IA Metrics Overview
- ISO/IEC 21827 (SSE-CMM) Overview
- Applying IA metrics to ISO/IEC 21827 to use as an Assurance Framework



IA Metrics/Performance Management is a recently established discipline

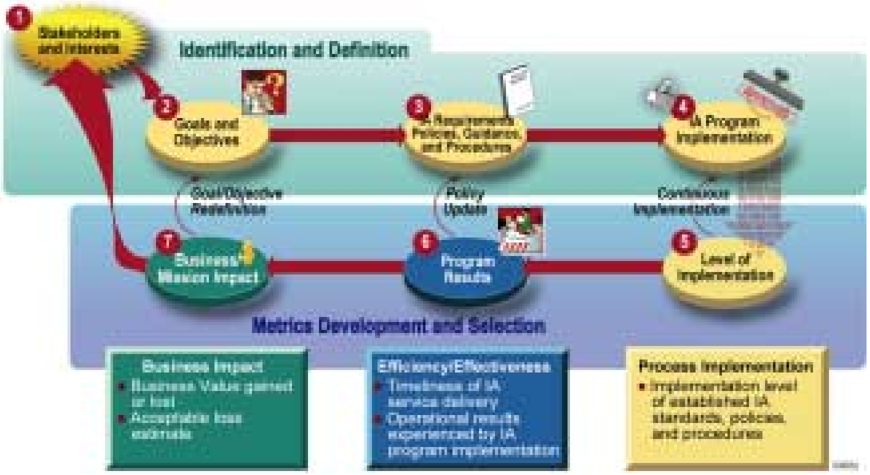
- Information Assurance Technology Analysis Center (IATAC) IA Metrics Report, May 2000
- Chairman, Joint Chiefs of Staff Instructions (CJCSI)
  - CJCSI 6510.04, Information Assurance (IA) Readiness Metrics, May 2000, canceled by
  - CJCSI IA and Computer Network Defense (CND) Joint Quarterly Readiness Review Metrics, CJCSI 3401.03, October 2002
- Laws
  - Government Information Security Reform Act (GISRA), October 2000, superceded by
  - Federal Information Security Management Act (FISMA), E-government Act, Title III, December 2002
- NIST
  - Information Technology (IT) Security Metrics Workshop, May 2002
  - NIST Special Publication (SP) 800-55, Security Metrics Guide for IT Systems, July 2003
- International Organization for Standardization (ISO) is in the process of developing Information Security Metrics and Measurements Standard (ISO/IEC27004)



IA Metrics can be used for multiple purposes

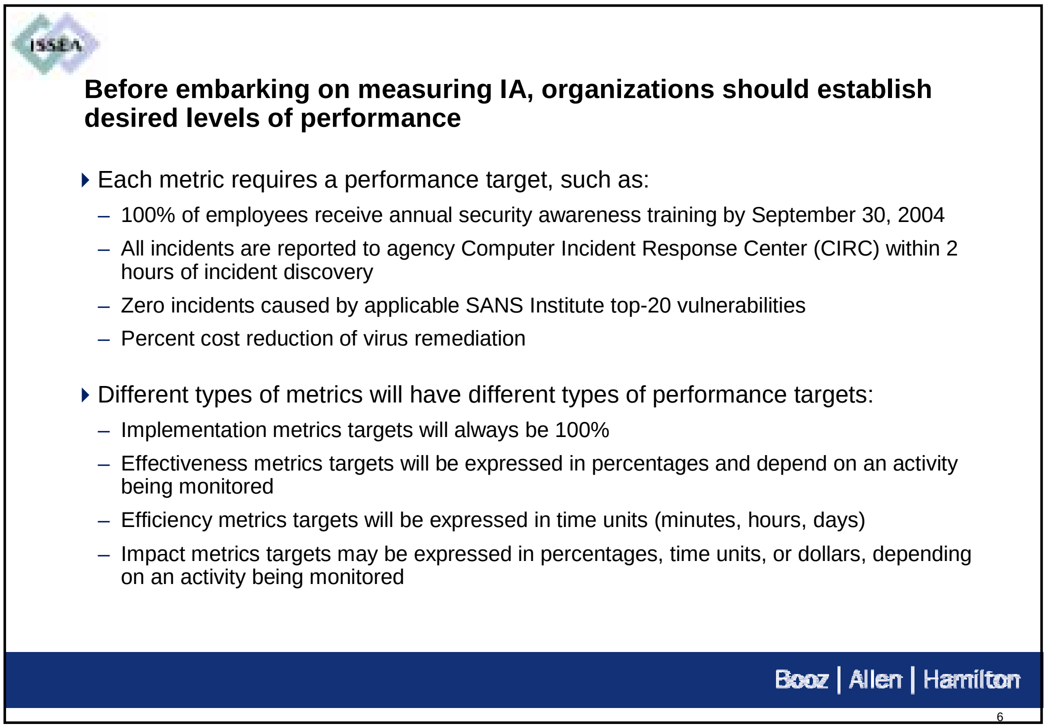
- Improving effectiveness and efficiency of your organization’s IA program
  - Create a feedback loop for monitoring implementation of your organization’s IA policies, processes, and procedures
  - Determine whether IA policies, processes, and procedures accomplish the goal of appropriately protecting your organization’s assets
  - Create a roadmap for IA program improvement based on quantifiable performance feedback
- Convincing your management that IA is creating value for the organization
  - Provide a solid baseline for business case development
  - Provide objective information for investment selection, control, and evaluation
- Reducing regulatory reporting burden
  - Implement efficient data collection processes to collect data once and use it for multiple reports
- Validating baseline capability levels and monitoring changes over time
- Quantifying assurance arguments

Organizations need multiple types of metrics to monitor their IA performance


1
Stakeholders and Interests
Identification and Definition
2
Goals and Objectives
3
IA Requirements Policies, Guidance, and Procedures
4
IA Program Implementation
Goal/Objective Redefinition
Policy Update
Continuous Implementation
7
Business/ Mission Impact
6
Program Results
5
Level of Implementation
Metrics Development and Selection
Business Impact
Business Value gained or lost
Acceptable loss estimate
Efficiency/Effectiveness
Timeliness of IA service delivery
Operational results experienced by IA program implementation
Process Implementation
Implementation level of established IA standards, policies, and procedures

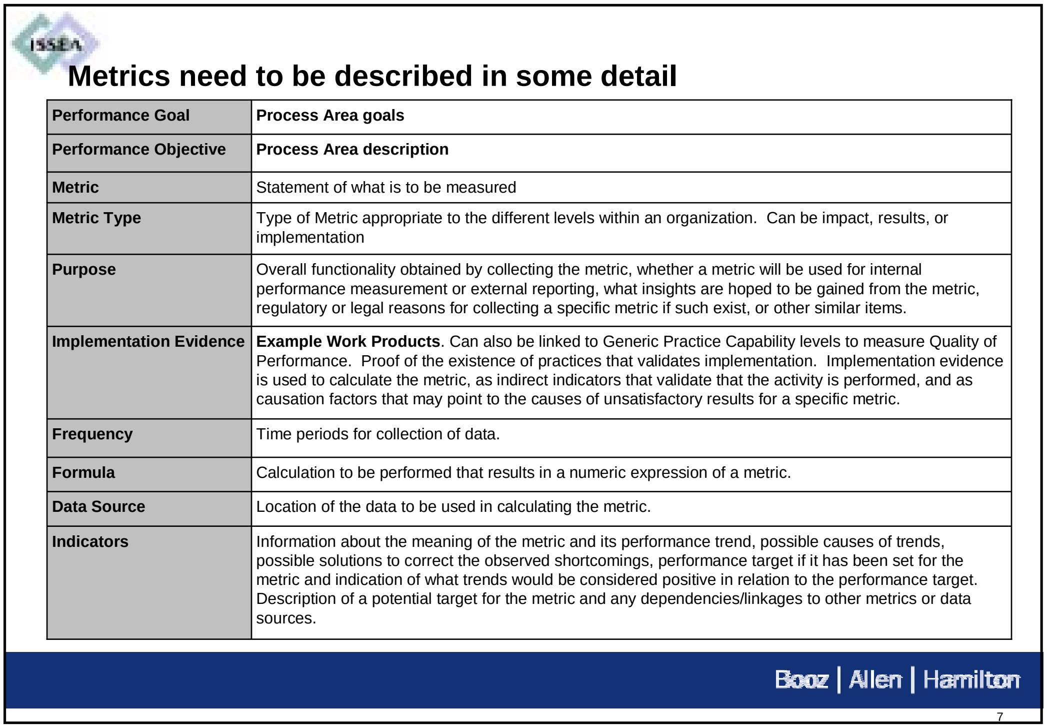
Metrics Examples

Implementation	Percentage of assets identified and prioritized for criticality Existence of assurance objectives (yes/no)
Efficiency/effectiveness	Percent of registered unexpected and unwanted events Speed of event response (reaction time) Time to regain operational status after unscheduled downtime Assurance evidence age (appropriate for and in relation to activity) Accessibility of evidence (how easy is it to extract evidence out of a process and make it available) Timeliness of assurance argument
Business or mission impact	Cost of event response (per event) Units of time to regain 100% operational capability Variance between planned and actual spending on training-related activities



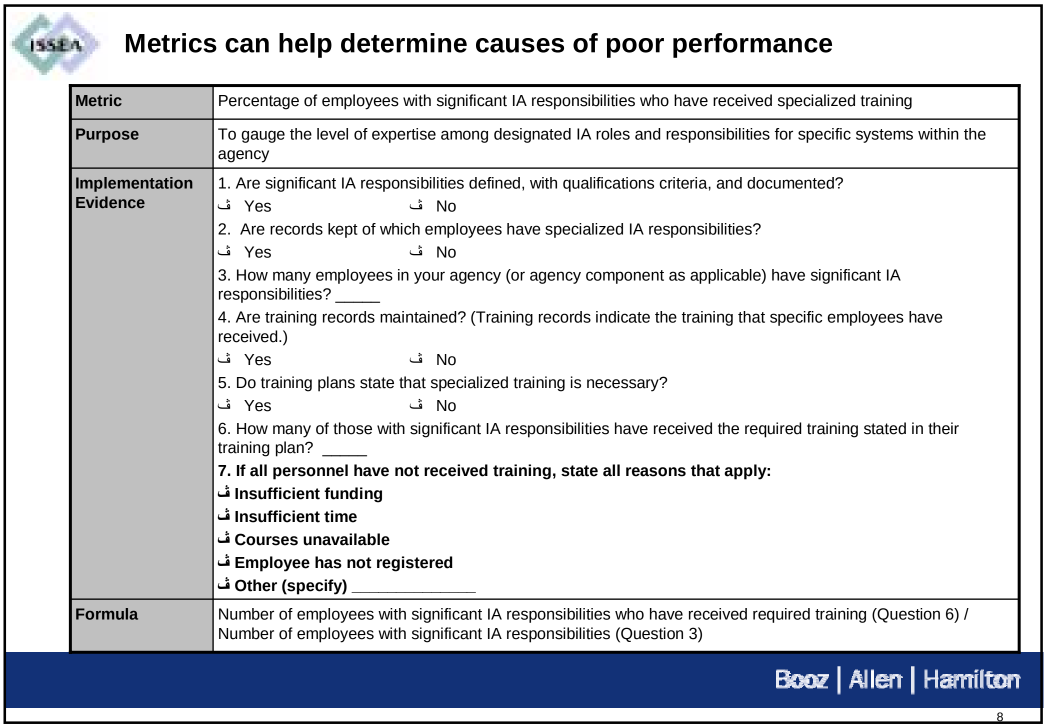
Before embarking on measuring IA, organizations should establish desired levels of performance

- Each metric requires a performance target, such as:
  - 100% of employees receive annual security awareness training by September 30, 2004
  - All incidents are reported to agency Computer Incident Response Center (CIRC) within 2 hours of incident discovery
  - Zero incidents caused by applicable SANS Institute top-20 vulnerabilities
  - Percent cost reduction of virus remediation
- Different types of metrics will have different types of performance targets:
  - Implementation metrics targets will always be 100%
  - Effectiveness metrics targets will be expressed in percentages and depend on an activity being monitored
  - Efficiency metrics targets will be expressed in time units (minutes, hours, days)
  - Impact metrics targets may be expressed in percentages, time units, or dollars, depending on an activity being monitored



Metrics need to be described in some detail

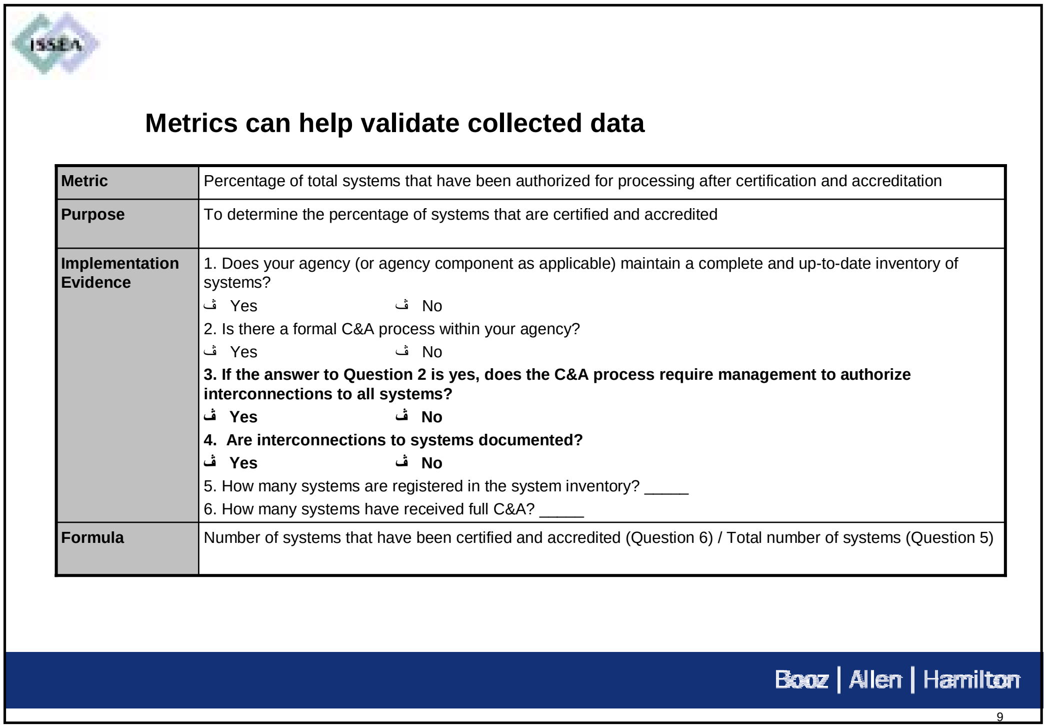
Performance Goal	**Process Area goals**
Performance Objective	**Process Area description**
Metric	Statement of what is to be measured
Metric Type	Type of Metric appropriate to the different levels within an organization. Can be impact, results, or implementation
Purpose	Overall functionality obtained by collecting the metric, whether a metric will be used for internal performance measurement or external reporting, what insights are hoped to be gained from the metric, regulatory or legal reasons for collecting a specific metric if such exist, or other similar items.
Implementation Evidence	**Example Work Products**. Can also be linked to Generic Practice Capability levels to measure Quality of Performance. Proof of the existence of practices that validates implementation. Implementation evidence is used to calculate the metric, as indirect indicators that validate that the activity is performed, and as causation factors that may point to the causes of unsatisfactory results for a specific metric.
Frequency	Time periods for collection of data.
Formula	Calculation to be performed that results in a numeric expression of a metric.
Data Source	Location of the data to be used in calculating the metric.
Indicators	Information about the meaning of the metric and its performance trend, possible causes of trends, possible solutions to correct the observed shortcomings, performance target if it has been set for the metric and indication of what trends would be considered positive in relation to the performance target. Description of a potential target for the metric and any dependencies/linkages to other metrics or data sources.



Metrics can help determine causes of poor performance

Metric	Percentage of employees with significant IA responsibilities who have received specialized training
Purpose	To gauge the level of expertise among designated IA roles and responsibilities for specific systems within the agency
Implementation Evidence	1. Are significant IA responsibilities defined, with qualifications criteria, and documented? □ Yes □ No 2. Are records kept of which employees have specialized IA responsibilities? □ Yes □ No 3. How many employees in your agency (or agency component as applicable) have significant IA responsibilities? _____ 4. Are training records maintained? (Training records indicate the training that specific employees have received.) □ Yes □ No 5. Do training plans state that specialized training is necessary? □ Yes □ No 6. How many of those with significant IA responsibilities have received the required training stated in their training plan? _____ **7. If all personnel have not received training, state all reasons that apply:** **□ Insufficient funding** **□ Insufficient time** **□ Courses unavailable** **□ Employee has not registered** **□ Other (specify) _______________**
Formula	Number of employees with significant IA responsibilities who have received required training (Question 6) / Number of employees with significant IA responsibilities (Question 3)

Booz | Allen | Hamilton



Metrics can help validate collected data

Metric	Percentage of total systems that have been authorized for processing after certification and accreditation
Purpose	To determine the percentage of systems that are certified and accredited
Implementation Evidence	1. Does your agency (or agency component as applicable) maintain a complete and up-to-date inventory of systems? □ Yes □ No 2. Is there a formal C&A process within your agency? □ Yes □ No **3. If the answer to Question 2 is yes, does the C&A process require management to authorize interconnections to all systems?** **□ Yes □ No** **4. Are interconnections to systems documented?** **□ Yes □ No** 5. How many systems are registered in the system inventory? _____ 6. How many systems have received full C&A? _____
Formula	Number of systems that have been certified and accredited (Question 6) / Total number of systems (Question 5)

Booz | Allen | Hamilton

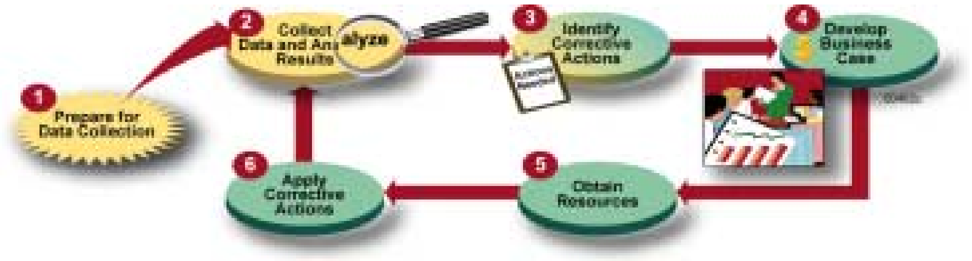
IA Metrics implementation is an iterative process

- Identify stakeholders
- Determine goals/objectives
- Review existing metrics
- Develop new metrics
- Identify data collection methods and tools

- Collect metrics data
- Analyze collected data
- Identify gaps between actual and desired performance
- Identify reasons for undesired results
- Identify areas requiring improvement

- Determine range of corrective actions
- Select most appropriate corrective actions
- Prioritize corrective actions based on overall risk mitigation goals

- Develop cost model
  - Project cost for each corrective action
- Perform sensitivity analysis
- Develop business case
- Prepare budget submission

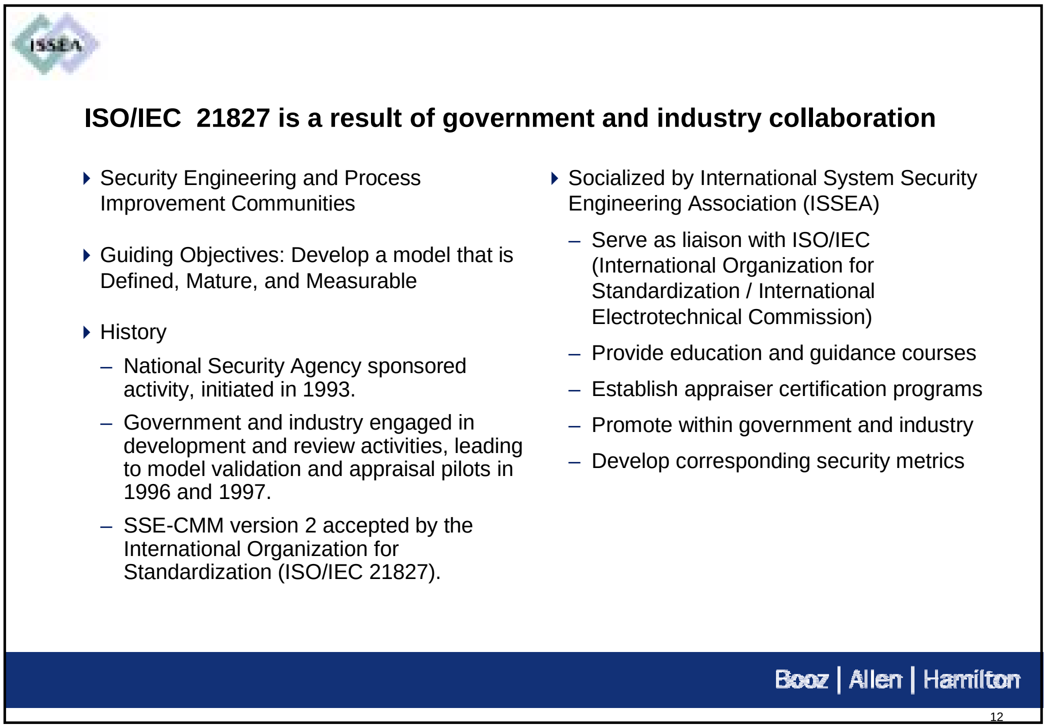

1 Prepare for Data Collection
2 Collect Data and Analyze Results
3 Identify Corrective Actions
4 Develop Business Case
5 Obtain Resources
6 Apply Corrective Actions

- Management
- Technical
- Operational

- Budget allocated
- Available resources prioritized
- Resources assigned

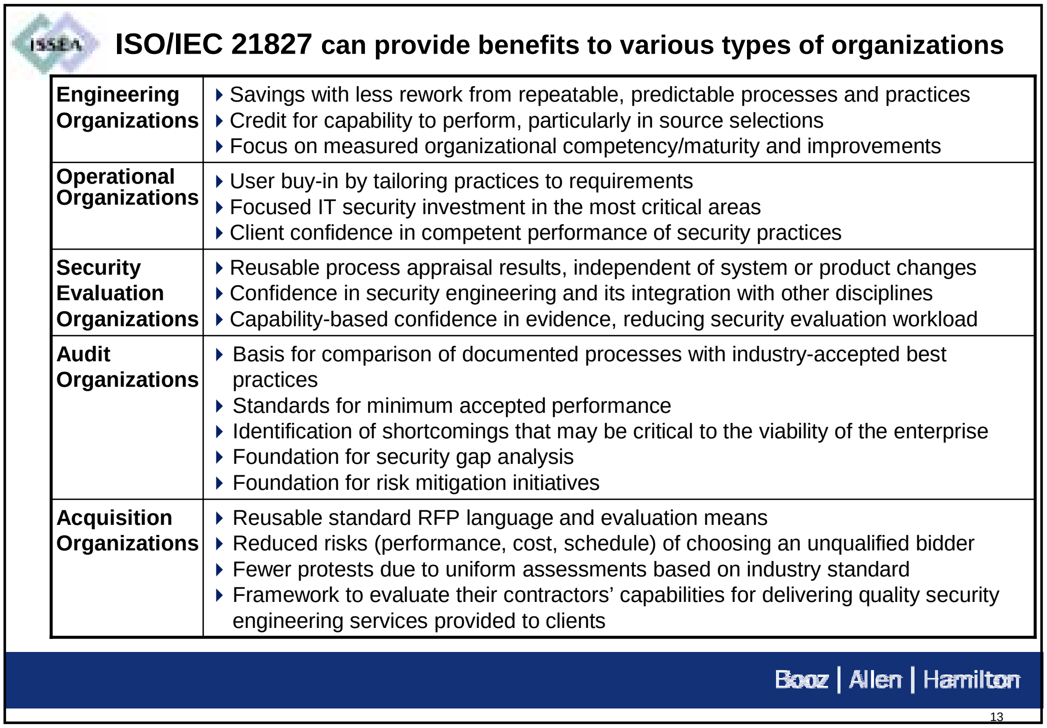
When applied to ISO/IEC 21827 IA Metrics provide a powerful process improvement tool

- Link security practice performance to business and IA goals
- Quantify compliance with standards
- Measure effectiveness and efficiency of IA implementation for a particular organization
- Identify data used for measurement
- Repeat measurement to provide relevant performance trends over time
- Identify opportunities for corrective actions leading to formulation of action plans
- Support IA improvement and budget recommendations
- Produce evidence that substantiates assurance argument



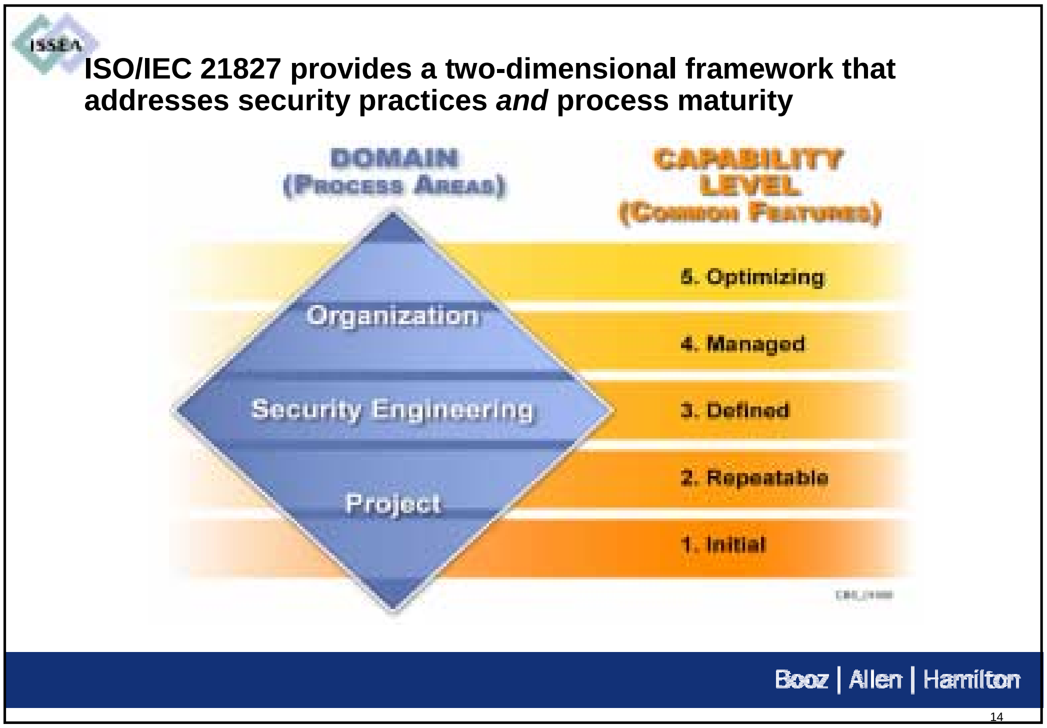
ISO/IEC 21827 is a result of government and industry collaboration

- Security Engineering and Process Improvement Communities
- Guiding Objectives: Develop a model that is Defined, Mature, and Measurable
- History
  - National Security Agency sponsored activity, initiated in 1993.
  - Government and industry engaged in development and review activities, leading to model validation and appraisal pilots in 1996 and 1997.
  - SSE-CMM version 2 accepted by the International Organization for Standardization (ISO/IEC 21827).
- Socialized by International System Security Engineering Association (ISSEA)
  - Serve as liaison with ISO/IEC (International Organization for Standardization / International Electrotechnical Commission)
  - Provide education and guidance courses
  - Establish appraiser certification programs
  - Promote within government and industry
  - Develop corresponding security metrics



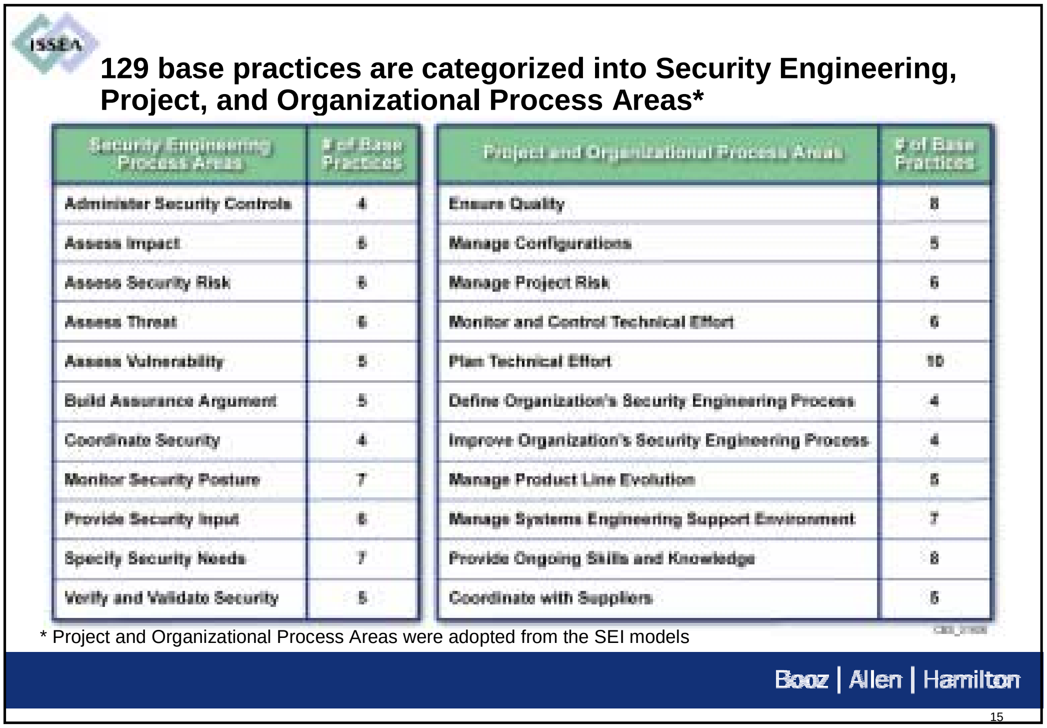
ISO/IEC 21827 can provide benefits to various types of organizations

Engineering Organizations	Savings with less rework from repeatable, predictable processes and practices Credit for capability to perform, particularly in source selections Focus on measured organizational competency/maturity and improvements
Operational Organizations	User buy-in by tailoring practices to requirements Focused IT security investment in the most critical areas Client confidence in competent performance of security practices
Security Evaluation Organizations	Reusable process appraisal results, independent of system or product changes Confidence in security engineering and its integration with other disciplines Capability-based confidence in evidence, reducing security evaluation workload
Audit Organizations	Basis for comparison of documented processes with industry-accepted best practices Standards for minimum accepted performance Identification of shortcomings that may be critical to the viability of the enterprise Foundation for security gap analysis Foundation for risk mitigation initiatives
Acquisition Organizations	Reusable standard RFP language and evaluation means Reduced risks (performance, cost, schedule) of choosing an unqualified bidder Fewer protests due to uniform assessments based on industry standard Framework to evaluate their contractors' capabilities for delivering quality security engineering services provided to clients



ISO/IEC 21827 provides a two-dimensional framework that addresses security practices *and* process maturity

Booz | Allen | Hamilton



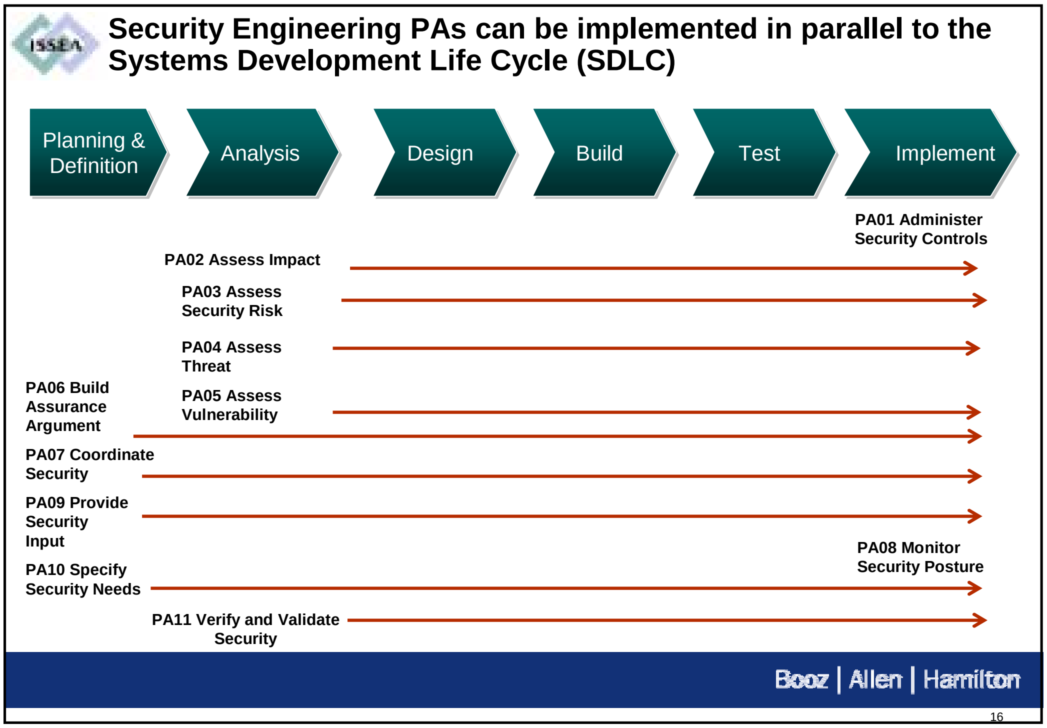
129 base practices are categorized into Security Engineering, Project, and Organizational Process Areas*

Security Engineering Process Areas	# of Base Practices
Administer Security Controls	4
Assess Impact	6
Assess Security Risk	6
Assess Threat	6
Assess Vulnerability	5
Build Assurance Argument	5
Coordinate Security	4
Monitor Security Posture	7
Provide Security Input	6
Specify Security Needs	7
Verify and Validate Security	5

Project and Organizational Process Areas	# of Base Practices
Ensure Quality	8
Manage Configurations	5
Manage Project Risk	6
Monitor and Control Technical Effort	6
Plan Technical Effort	10
Define Organization's Security Engineering Process	4
Improve Organization's Security Engineering Process	4
Manage Product Line Evolution	5
Manage Systems Engineering Support Environment	7
Provide Ongoing Skills and Knowledge	8
Coordinate with Suppliers	6

* Project and Organizational Process Areas were adopted from the SEI models

Booz | Allen | Hamilton



Security Engineering PAs can be implemented in parallel to the Systems Development Life Cycle (SDLC)

Planning & Definition → Analysis → Design → Build → Test → Implement

PA01 Administer Security Controls

PA02 Assess Impact

PA03 Assess Security Risk

PA04 Assess Threat

PA05 Assess Vulnerability

PA06 Build Assurance Argument

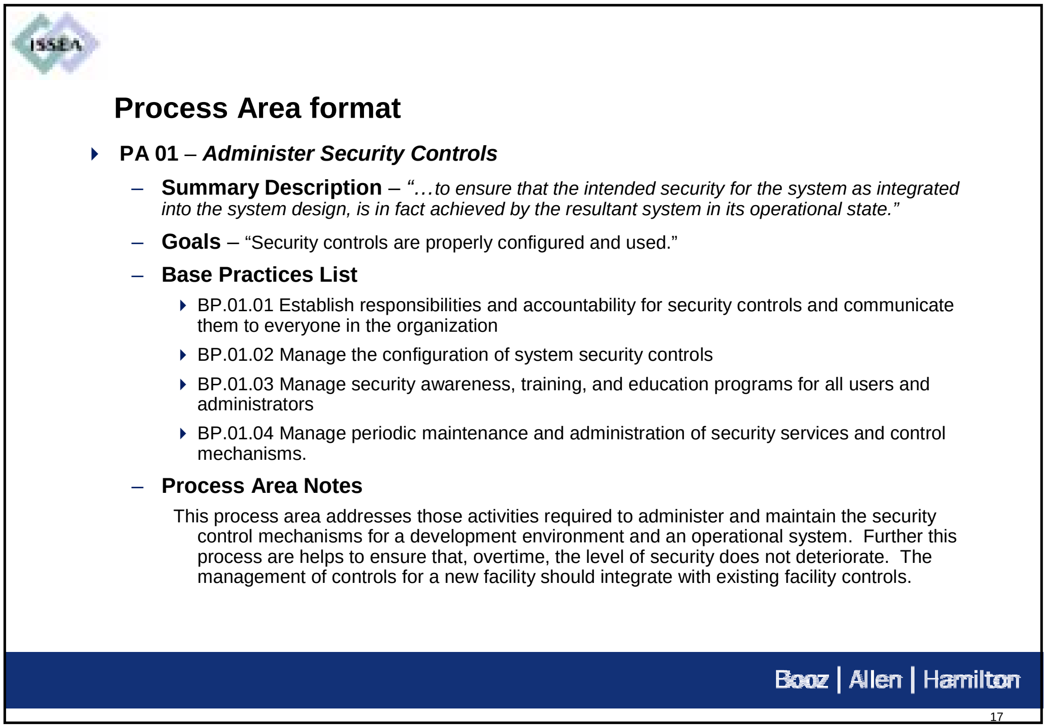
PA07 Coordinate Security

PA09 Provide Security Input

PA08 Monitor Security Posture

PA10 Specify Security Needs

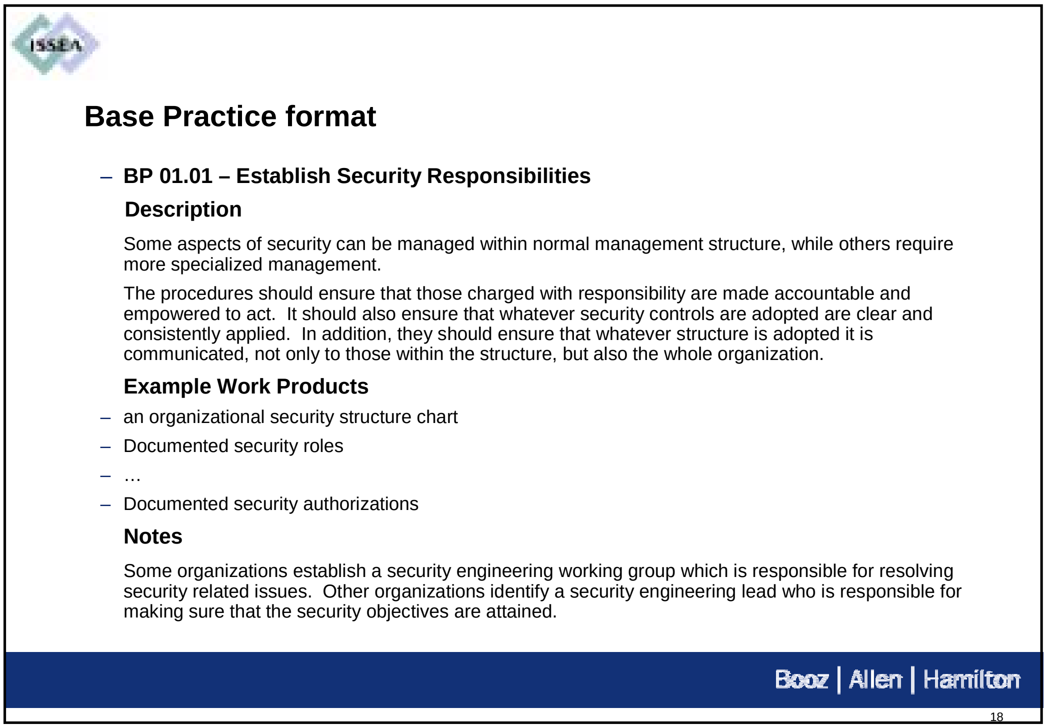
PA11 Verify and Validate Security



Process Area format

- **PA 01** – ***Administer Security Controls***
  - **Summary Description** – *"…to ensure that the intended security for the system as integrated into the system design, is in fact achieved by the resultant system in its operational state."*
  - **Goals** – "Security controls are properly configured and used."
  - **Base Practices List**
    - BP.01.01 Establish responsibilities and accountability for security controls and communicate them to everyone in the organization
    - BP.01.02 Manage the configuration of system security controls
    - BP.01.03 Manage security awareness, training, and education programs for all users and administrators
    - BP.01.04 Manage periodic maintenance and administration of security services and control mechanisms.
  - **Process Area Notes**

    This process area addresses those activities required to administer and maintain the security control mechanisms for a development environment and an operational system. Further this process are helps to ensure that, overtime, the level of security does not deteriorate. The management of controls for a new facility should integrate with existing facility controls.



Base Practice format

- **BP 01.01 – Establish Security Responsibilities**

Description

Some aspects of security can be managed within normal management structure, while others require more specialized management.

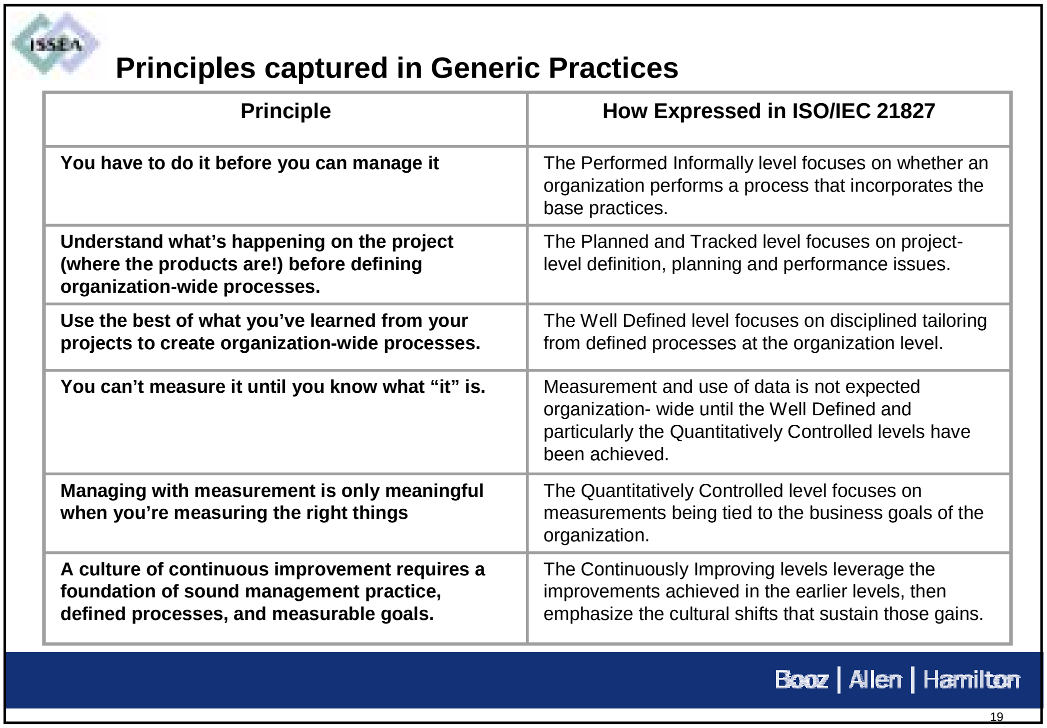
The procedures should ensure that those charged with responsibility are made accountable and empowered to act. It should also ensure that whatever security controls are adopted are clear and consistently applied. In addition, they should ensure that whatever structure is adopted it is communicated, not only to those within the structure, but also the whole organization.

Example Work Products

- an organizational security structure chart
- Documented security roles
- …
- Documented security authorizations

Notes

Some organizations establish a security engineering working group which is responsible for resolving security related issues. Other organizations identify a security engineering lead who is responsible for making sure that the security objectives are attained.

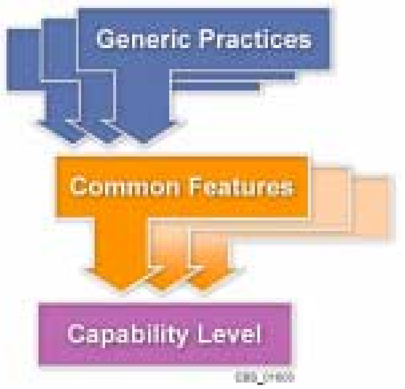


Principles captured in Generic Practices

Principle	How Expressed in ISO/IEC 21827
You have to do it before you can manage it	The Performed Informally level focuses on whether an organization performs a process that incorporates the base practices.
Understand what's happening on the project (where the products are!) before defining organization-wide processes.	The Planned and Tracked level focuses on project-level definition, planning and performance issues.
Use the best of what you've learned from your projects to create organization-wide processes.	The Well Defined level focuses on disciplined tailoring from defined processes at the organization level.
You can't measure it until you know what "it" is.	Measurement and use of data is not expected organization- wide until the Well Defined and particularly the Quantitatively Controlled levels have been achieved.
Managing with measurement is only meaningful when you're measuring the right things	The Quantitatively Controlled level focuses on measurements being tied to the business goals of the organization.
A culture of continuous improvement requires a foundation of sound management practice, defined processes, and measurable goals.	The Continuously Improving levels leverage the improvements achieved in the earlier levels, then emphasize the cultural shifts that sustain those gains.

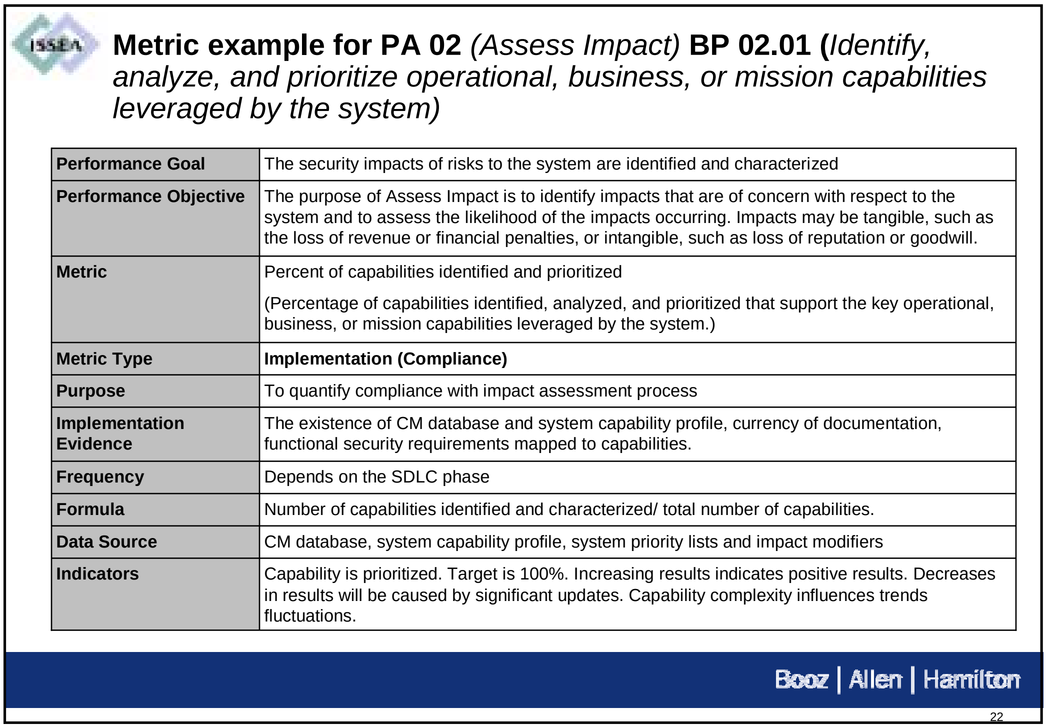
Generic Practices examples

- Capability Level 1- Performed Informally
- Common Feature 1.1- Base Practices are Performed
- **Generic Practice GP 1.1.1** Perform the Process
  - Perform a process that implements the base practices of the process area to provide work products and/or s to a customer.
- Capability Level 3- Well Defined
- Common Feature 3.1- Defining a Standard Process
- **Generic Practice GP 3.1.1** Standardize the Process
  - Document a standard process or family of processes for the organization, that describes how to implement the base practices of the process area
- **Generic Practice GP 3.1.2** Tailor the Standard Process
  - Tailor the organization’s standard process family to create a defined process that addresses the particular needs of a specific use.



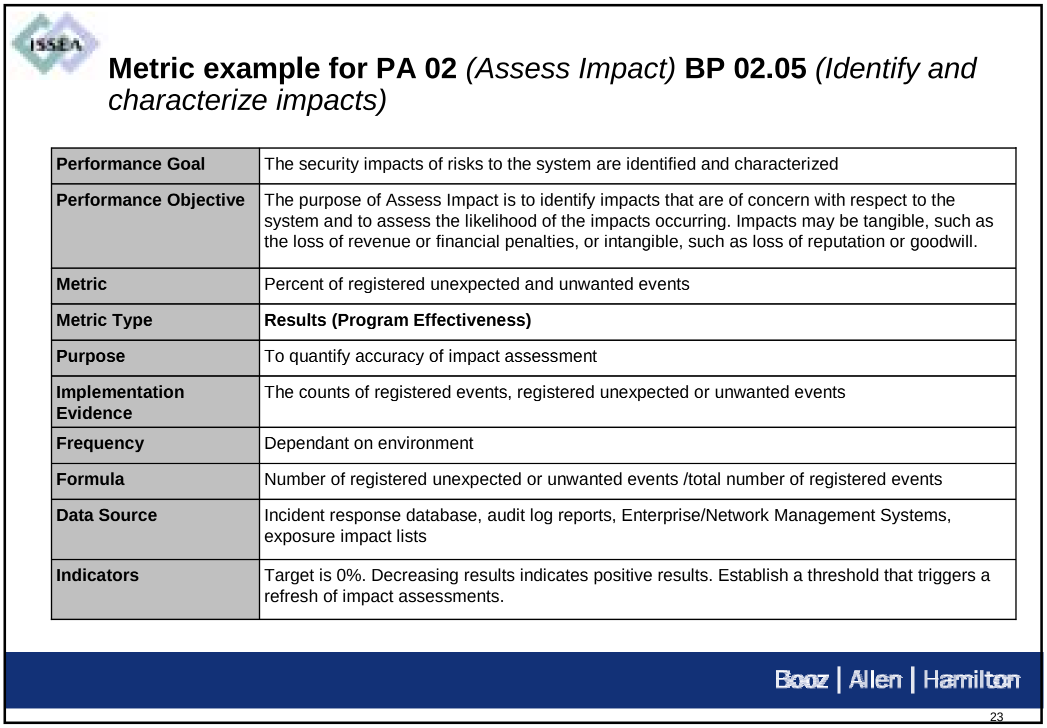
ISSEA recently completed development of ISO/IEC 21827 metrics

- To be used in conjunction with the model
- Measuring Process Area accomplishment (compliance), effectiveness, and impact
- Using a modified NIST SP 800-55 approach
- Provide at least 3 candidate metrics for each security PA
- Metrics are tailorable to each organization/project/program requirements and can be used with or without ISO/IEC 21827



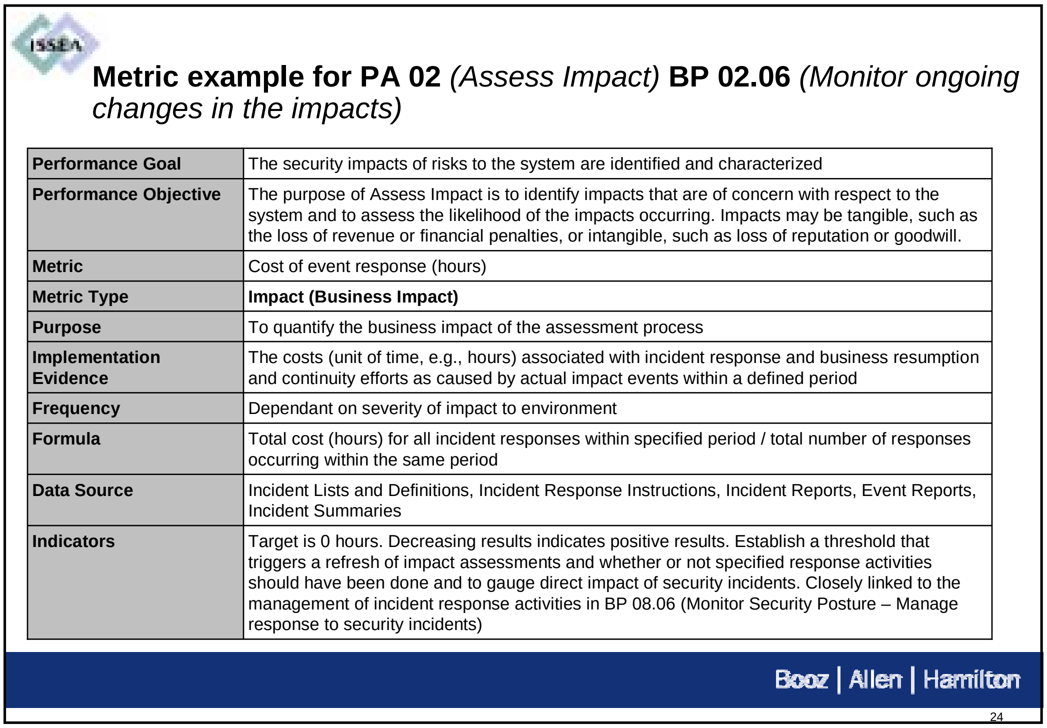
Metric example for PA 02 *(Assess Impact)* BP 02.01 (*Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system)*

Performance Goal	The security impacts of risks to the system are identified and characterized
Performance Objective	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible, such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.
Metric	Percent of capabilities identified and prioritized (Percentage of capabilities identified, analyzed, and prioritized that support the key operational, business, or mission capabilities leveraged by the system.)
Metric Type	**Implementation (Compliance)**
Purpose	To quantify compliance with impact assessment process
Implementation Evidence	The existence of CM database and system capability profile, currency of documentation, functional security requirements mapped to capabilities.
Frequency	Depends on the SDLC phase
Formula	Number of capabilities identified and characterized/ total number of capabilities.
Data Source	CM database, system capability profile, system priority lists and impact modifiers
Indicators	Capability is prioritized. Target is 100%. Increasing results indicates positive results. Decreases in results will be caused by significant updates. Capability complexity influences trends fluctuations.



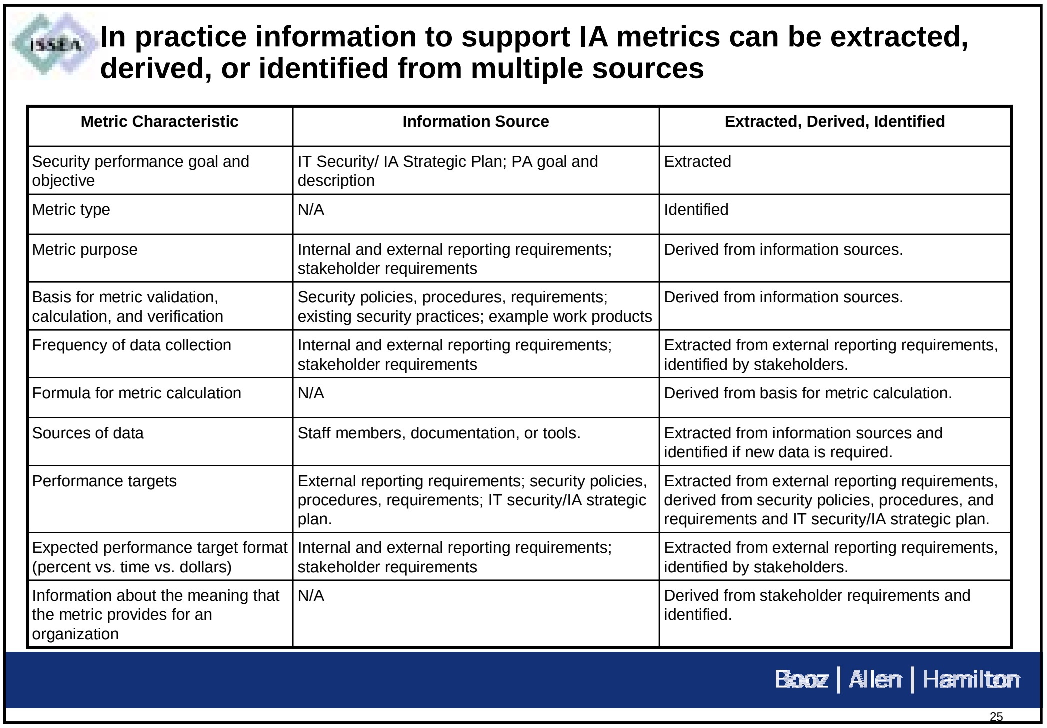
Metric example for PA 02 *(Assess Impact)* BP 02.05 *(Identify and characterize impacts)*

Performance Goal	The security impacts of risks to the system are identified and characterized
Performance Objective	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible, such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.
Metric	Percent of registered unexpected and unwanted events
Metric Type	**Results (Program Effectiveness)**
Purpose	To quantify accuracy of impact assessment
Implementation Evidence	The counts of registered events, registered unexpected or unwanted events
Frequency	Dependant on environment
Formula	Number of registered unexpected or unwanted events /total number of registered events
Data Source	Incident response database, audit log reports, Enterprise/Network Management Systems, exposure impact lists
Indicators	Target is 0%. Decreasing results indicates positive results. Establish a threshold that triggers a refresh of impact assessments.



Metric example for PA 02 *(Assess Impact)* BP 02.06 *(Monitor ongoing changes in the impacts)*

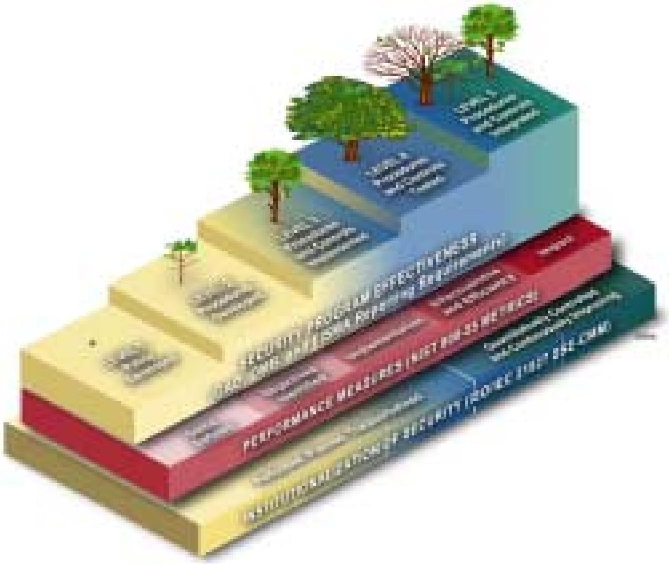
Performance Goal	The security impacts of risks to the system are identified and characterized
Performance Objective	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible, such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.
Metric	Cost of event response (hours)
Metric Type	**Impact (Business Impact)**
Purpose	To quantify the business impact of the assessment process
Implementation Evidence	The costs (unit of time, e.g., hours) associated with incident response and business resumption and continuity efforts as caused by actual impact events within a defined period
Frequency	Dependant on severity of impact to environment
Formula	Total cost (hours) for all incident responses within specified period / total number of responses occurring within the same period
Data Source	Incident Lists and Definitions, Incident Response Instructions, Incident Reports, Event Reports, Incident Summaries
Indicators	Target is 0 hours. Decreasing results indicates positive results. Establish a threshold that triggers a refresh of impact assessments and whether or not specified response activities should have been done and to gauge direct impact of security incidents. Closely linked to the management of incident response activities in BP 08.06 (Monitor Security Posture – Manage response to security incidents)



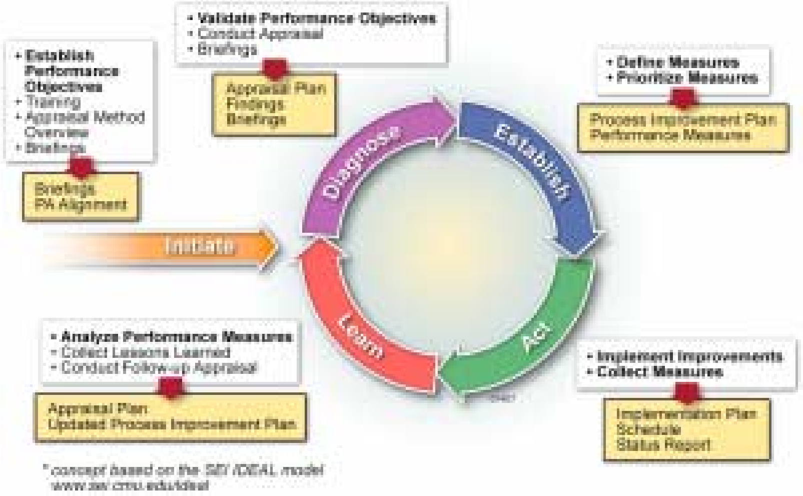
In practice information to support IA metrics can be extracted, derived, or identified from multiple sources

Metric Characteristic	Information Source	Extracted, Derived, Identified
Security performance goal and objective	IT Security/ IA Strategic Plan; PA goal and description	Extracted
Metric type	N/A	Identified
Metric purpose	Internal and external reporting requirements; stakeholder requirements	Derived from information sources.
Basis for metric validation, calculation, and verification	Security policies, procedures, requirements; existing security practices; example work products	Derived from information sources.
Frequency of data collection	Internal and external reporting requirements; stakeholder requirements	Extracted from external reporting requirements, identified by stakeholders.
Formula for metric calculation	N/A	Derived from basis for metric calculation.
Sources of data	Staff members, documentation, or tools.	Extracted from information sources and identified if new data is required.
Performance targets	External reporting requirements; security policies, procedures, requirements; IT security/IA strategic plan.	Extracted from external reporting requirements, derived from security policies, procedures, and requirements and IT security/IA strategic plan.
Expected performance target format (percent vs. time vs. dollars)	Internal and external reporting requirements; stakeholder requirements	Extracted from external reporting requirements, identified by stakeholders.
Information about the meaning that the metric provides for an organization	N/A	Derived from stakeholder requirements and identified.

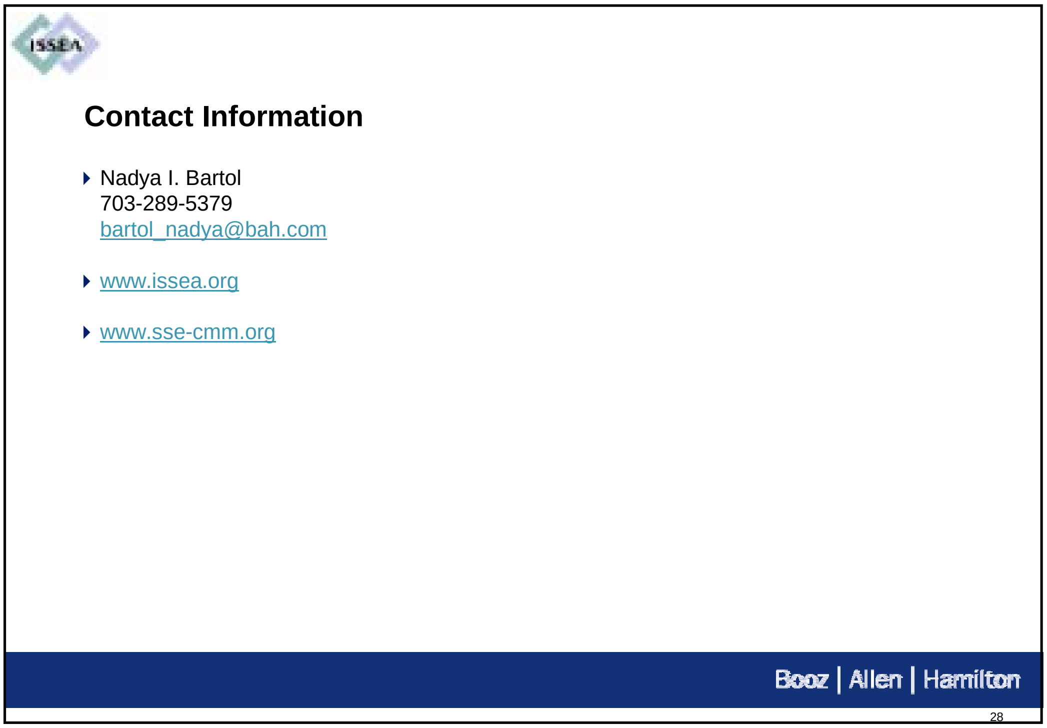
ISO/IEC 21827 provides a basis for establishing a comprehensive security program, coupled with robust security controls and metrics


SECURITY PROGRAM EFFECTIVENESS
PERFORMANCE MEASURES (NIST 800-55 METRICS)
INSTITUTIONALIZATION OF SECURITY (ISO/IEC 21827 SSE-CMM)
Impact

SEI IDEAL* approach can be used to effectively plan and manage ISO/IEC 21827 process improvement programs



* concept based on the SEI IDEAL model
www.sei.cmu.edu/ideal



Contact Information

- Nadya I. Bartol
  703-289-5379
  bartol_nadya@bah.com

- www.issea.org

- www.sse-cmm.org

Booz | Allen | Hamilton

28