AIRPORTS COUNCIL INTERNATIONAL

The voice of the world's airports

ACI World

Airport IT Security Benchmark initiative

Update to ACI-NA BIT Committee

ACI-NA Annual Conference & Exhibition | San Jose, CA

22 September 2013

Contents

Background

- Initiative of ACI World Airport IT Standing Committee
- Identified as a strategic priority by the ACI World Governing Board
- Service will allow airports to perform IT security self-assessments and benchmark their compliance against other airports
- ACI World will own and operate the system
- Planned official launch of the service: Q4 2013
  - Development of technical components almost complete
  - Draft of assessment questionnaire is ongoing

Airport IT Security Benchmark – the problem

- Airport operators need guidance to manage their IT Security risks
  - Increased dependency on IT
  - Emerging threats and growing points of vulnerability
  - Business Continuity requirements
  - Growing IT Security costs
  - Increased sophistication / coordinated attacks
  - Need for airports to collect and share information, guidance and best practice insight.
  - Identify strengths and weaknesses

Features

- Unique service tailored for airports
- Benchmark against peers (pax traffic, IT budget, ownership, etc.)
- Questionnaire based on a well-respected international standard
  - ISO 27002 provides best-practice recommendations
- Confidentiality of results
  - Only aggregated, anonymous data is provided as part of the benchmark
  - ACI will handle information requests among participants
- Graphical review of assessment results and compliance levels

Features

- Web-based
  - Self-assessments can be filled out online or on an iPad

ISO 27002 overview

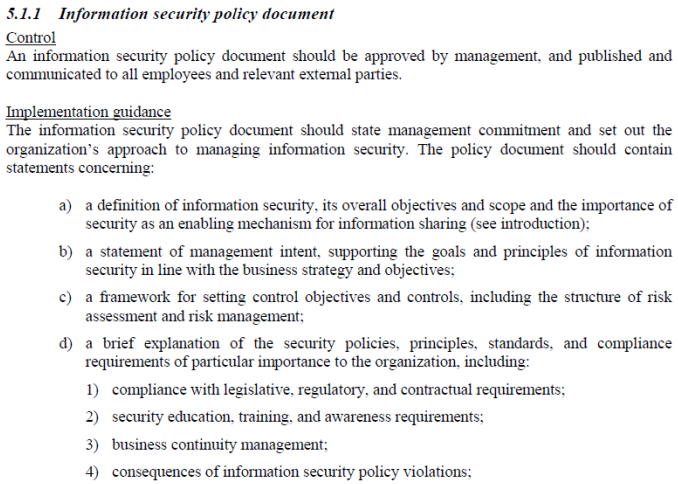
- 11 security control clauses
- 39 main security categories
- Each main security category contains:
  - A control objective stating what is to be achieved; and
  - One or more controls that can be applied to achieve the objective.

ISO 27002 control clauses

1. Security Policy;
2. Organizing Information Security;
3. Asset Management;
4. Human Resources Security;
5. Physical and Environmental Security;
6. Communications and Operations Management;
7. Access Control;
8. Information Systems Acquisition, Development and Maintenance;
9. Information Security Incident Management;
10. Business Continuity Management;
11. Compliance.

Assessment questionnaire

- Inspired by ISO 27002
  - Reduce scope of individual sections to facilitate benchmarking



5.1.1 Information security policy document

Control

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

Implementation guidance

The information security policy document should state management commitment and set out the organization's approach to managing information security. The policy document should contain statements concerning:

a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);

b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;

c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;

d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:

1) compliance with legislative, regulatory, and contractual requirements;

2) security education, training, and awareness requirements;

3) business continuity management;

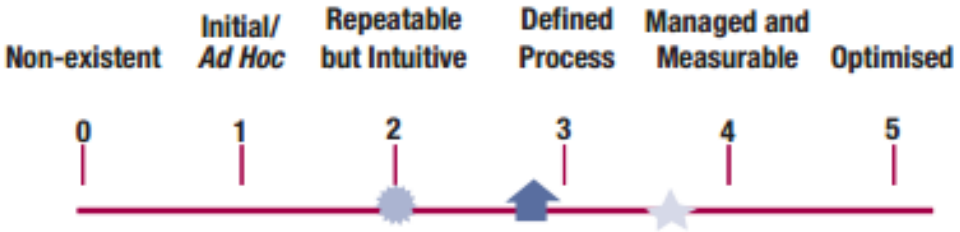
4) consequences of information security policy violations;

- Will be edited and revised as needed to suit airports

- Incorporate feedback from non-native English speakers

COBIT Maturity Model

Figure 12—Graphic Representation of Maturity Models



LEGEND FOR SYMBOLS USED

- Enterprise current status
- Industry average
- Enterprise target

LEGEND FOR RANKINGS USED

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

http://www.isaca.org

COBIT Maturity Model

Figure 13—Generic Maturity Model

0 Non-existent—Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.

1 Initial/*Ad Hoc*—There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.

2 Repeatable but Intuitive—Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

3 Defined Process—Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

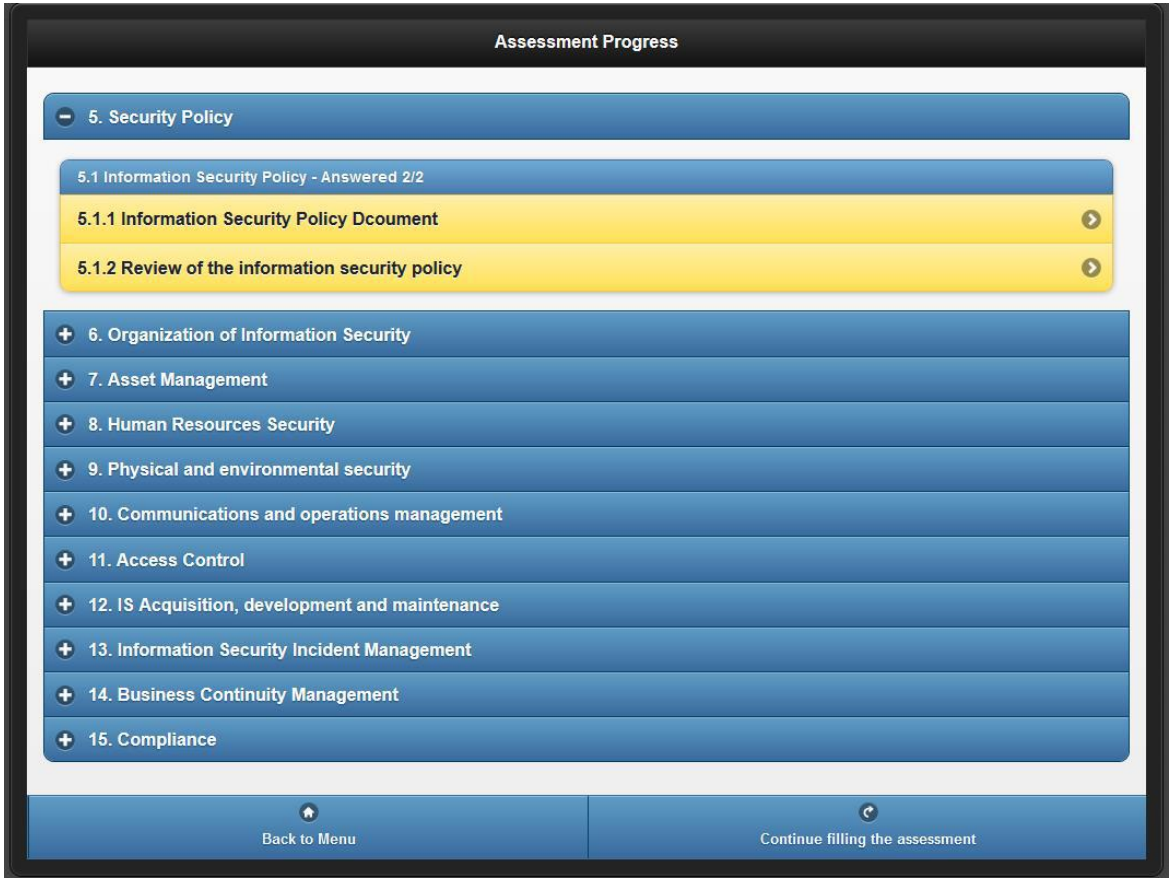
4 Managed and Measurable—Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 Optimised—Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

http://www.isaca.org

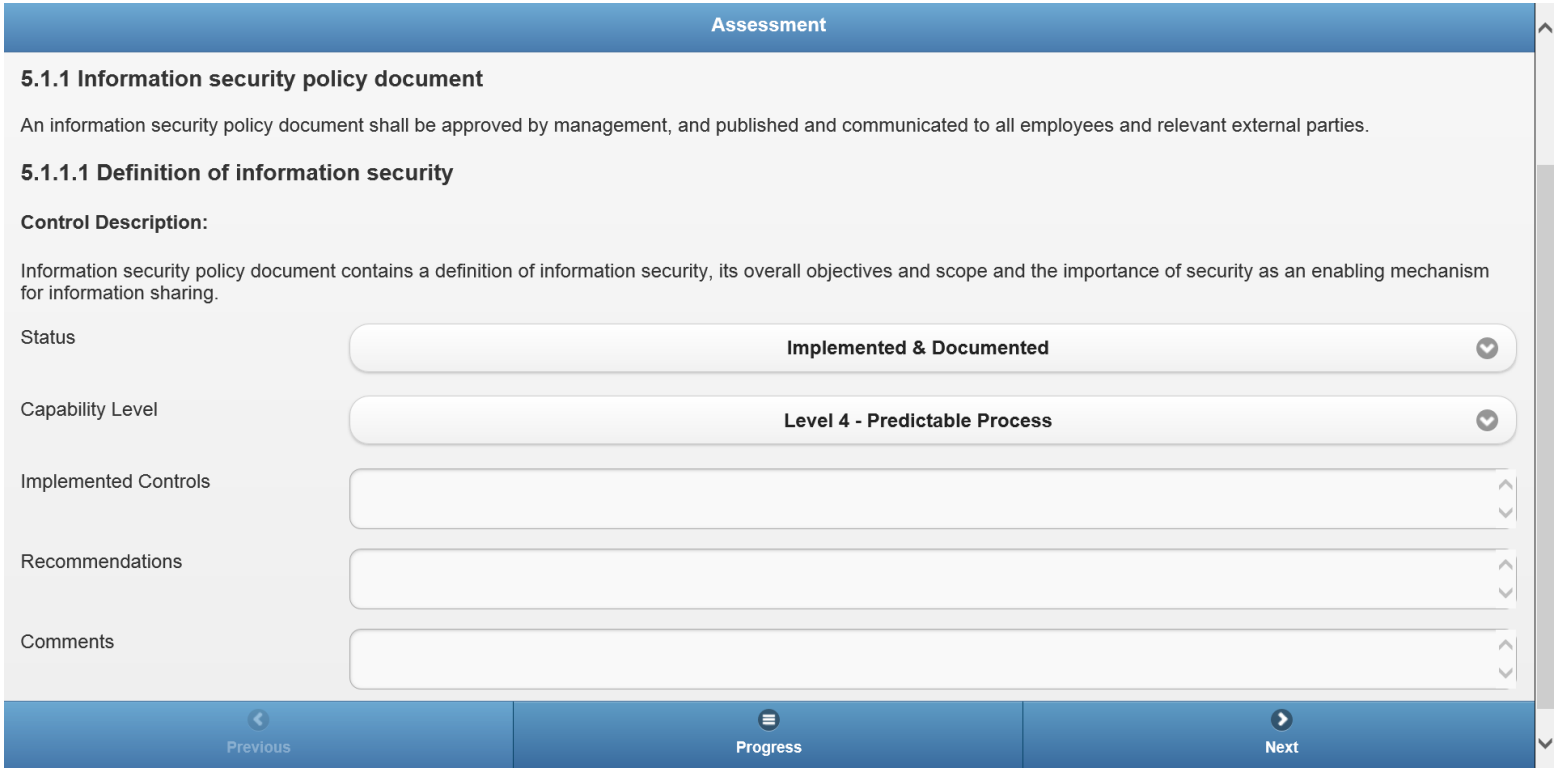
Airport IT Security Benchmark – solution overview

- Completing assessments



Airport IT Security Benchmark – solution overview

- Documenting compliance and maturity level



Airport IT Security Benchmark – solution overview

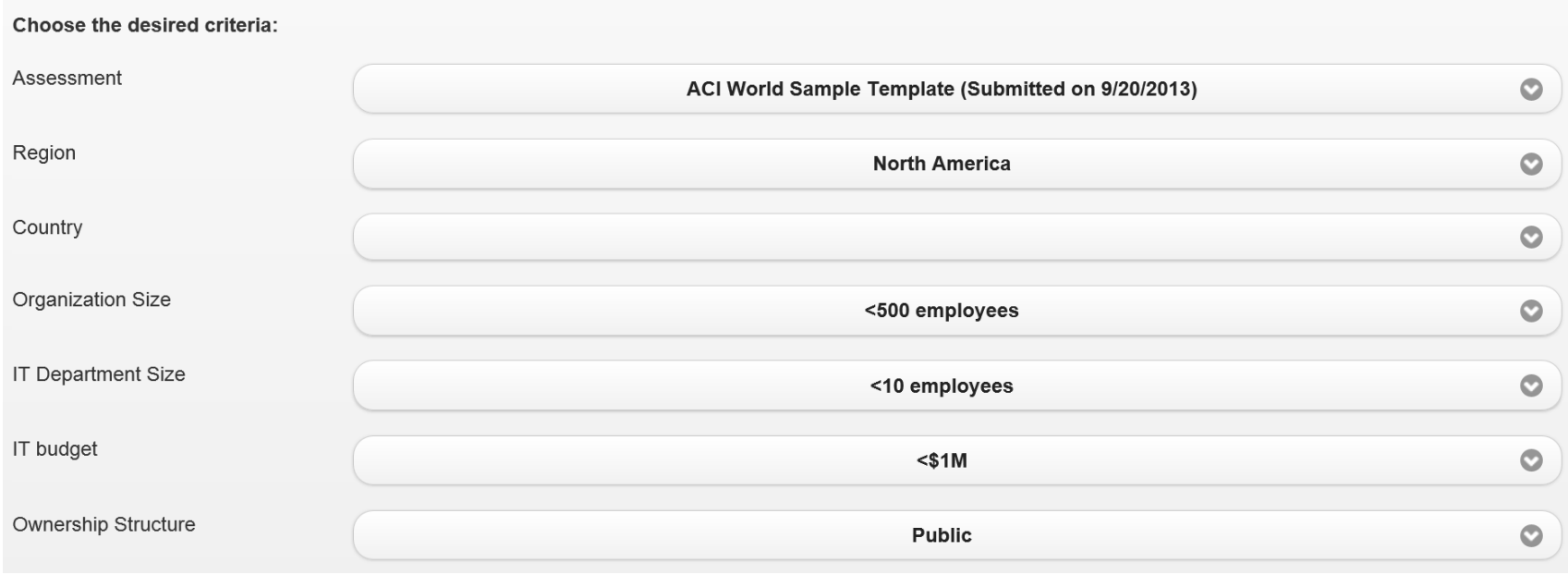
- Reviewing assessment results

Implementation Status based on ISO 27002

Section	Domain description	# Ctrls	Compliance %	Capability level	Description
5	Security Policy	2	100%	3	Established
6	Organization	11	100%	3	Established
7	Asset Management	5	80%	2	Managed
8	HR security	9	100%	3	Established
9	Physical and env security	13	100%	3	Established
10	Communications and operations mngt	32	100%	3	Established
11	Access Control	25	80%	2	Managed
12	IS acquisition, development and maintenance	5	100%	3	Established
13	IS incident management	5	50%	1	Performed
14	Business continuity management	5	100%	3	Established
15	Compliance	11	30%	0	Incomplete
		Results:	85%	Level 2	Managed

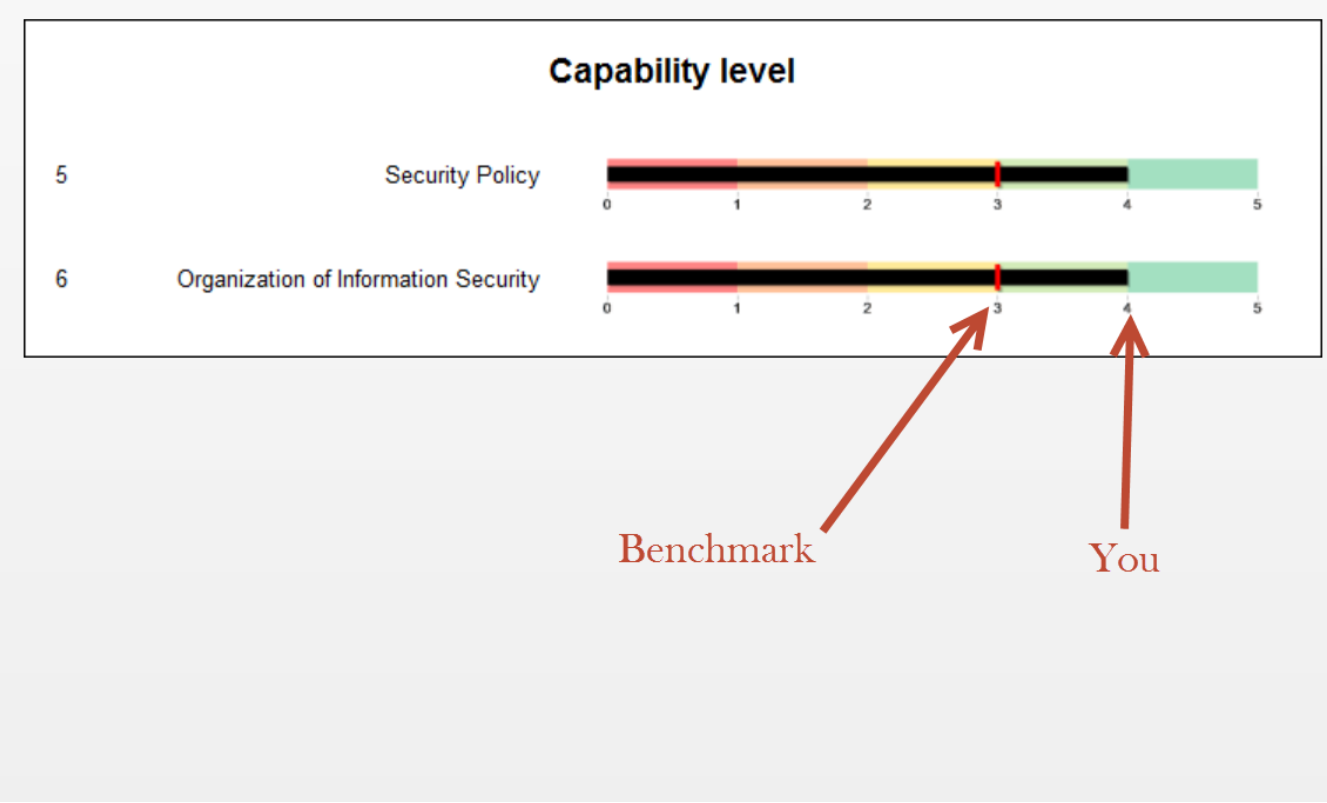
Airport IT Security Benchmark – solution overview

- Benchmark against peers



Airport IT Security Benchmark – solution overview

- Reviewing benchmark results



THANK YOU FOR YOUR ATTENTION!

www.aci.aero rabboud@aci.aero agarcia-alonso@aci.aero