

Fall ICSJWG 26 Oct 2010

ISA Security Compliance Institute Update

Johan Nye, ISCI Chairman (ExxonMobil)

Nate Kube, CTO, Wurldtech

Andre Ristaino, ASCI Managing Director (ISA)

*ISASecure*TM

www.isasecure.org

www.ansi.org/isasecure

Agenda

- ISA Security Compliance Institute (ISCI) Organization
- *ISASecure* Embedded Device Security Assurance Program
- Who to contact for more information
- Reference material



ISA Security Compliance Institute (ISCI) Organization

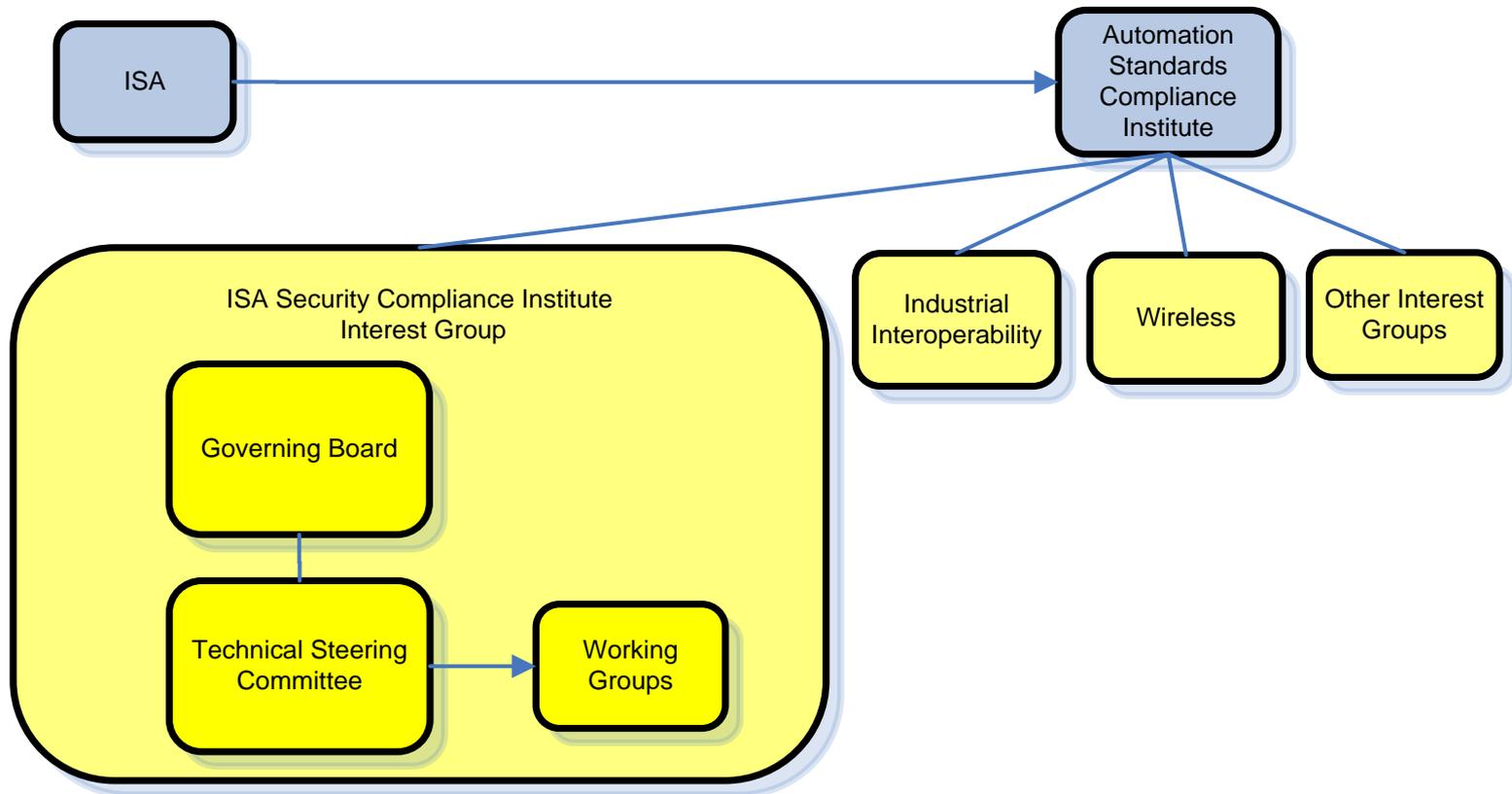
ISA Security Compliance Institute (ISCI)

Consortium of Asset Owners, Suppliers, and Industry Organizations formed in 2007 under the ISA Automation Standards Compliance Institute (ASCI) to:

Establish a set of well-engineered specifications and processes for the testing and certification of critical control systems products

Decrease the time, cost, and risk of developing, acquiring, and deploying control systems by establishing a collaborative industry-based program among asset owners, suppliers, and other stakeholders

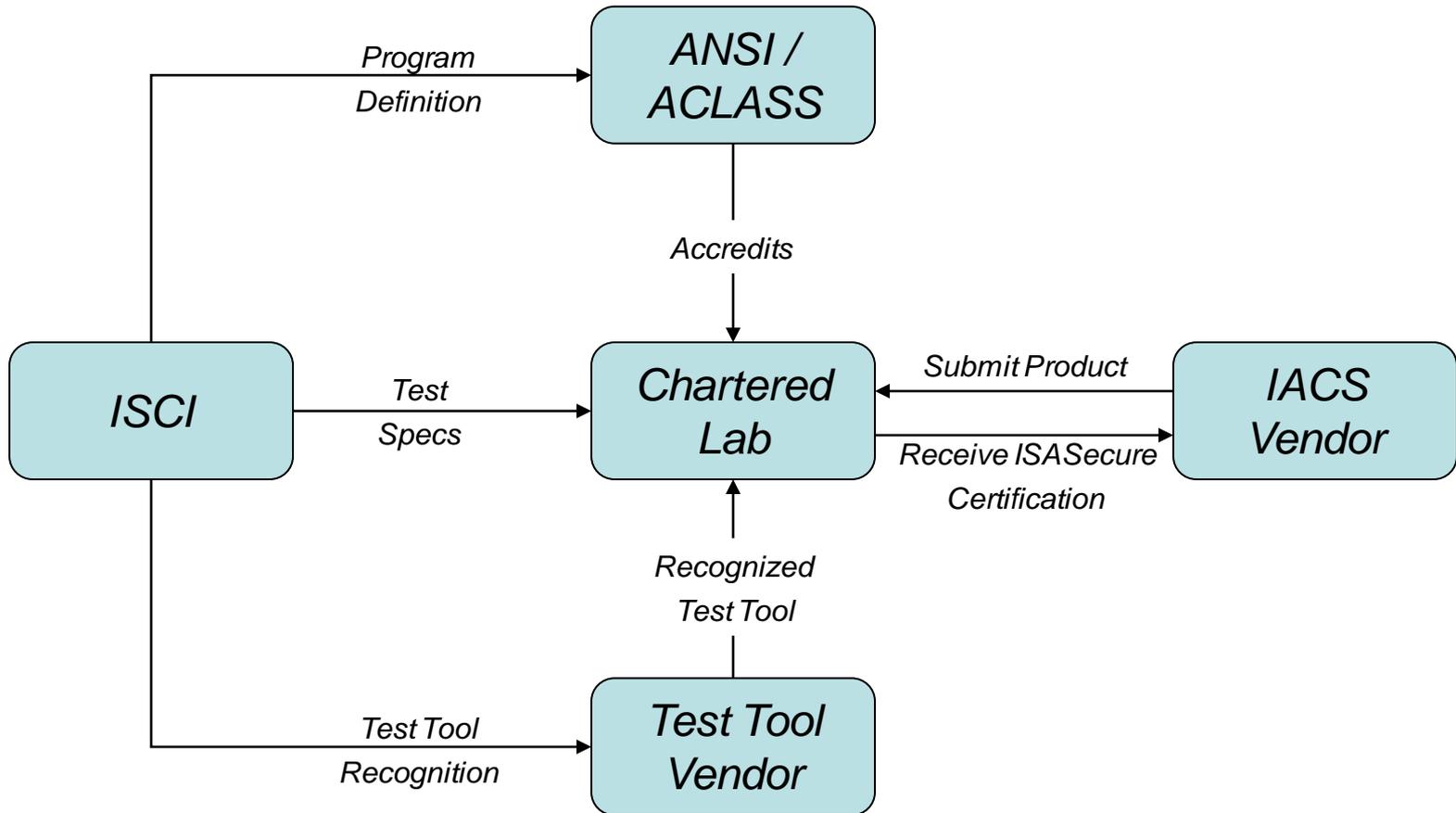
An ISA Owned Organization



ISCI Member Companies

- ISCI membership is open to all organizations
 - Strategic membership level
 - Technical membership level
 - Informational membership level
- Current membership
 - Chevron
 - Egemin
 - exida
 - ExxonMobil
 - Honeywell
 - Invensys
 - Mu Dynamics
 - Rockwell Automation
 - Siemens
 - Yokogawa
 - ISA99/ISCI Joint Working Group Liaison

ISASecure Program Relationships



ISASecure Designation



- Trademarked designation that provides instant recognition of product security characteristics and capabilities.
- Independent Industry stamp of approval.
- Similar to ‘Safety Integrity Level’ Certification (ISO/IEC 61508).

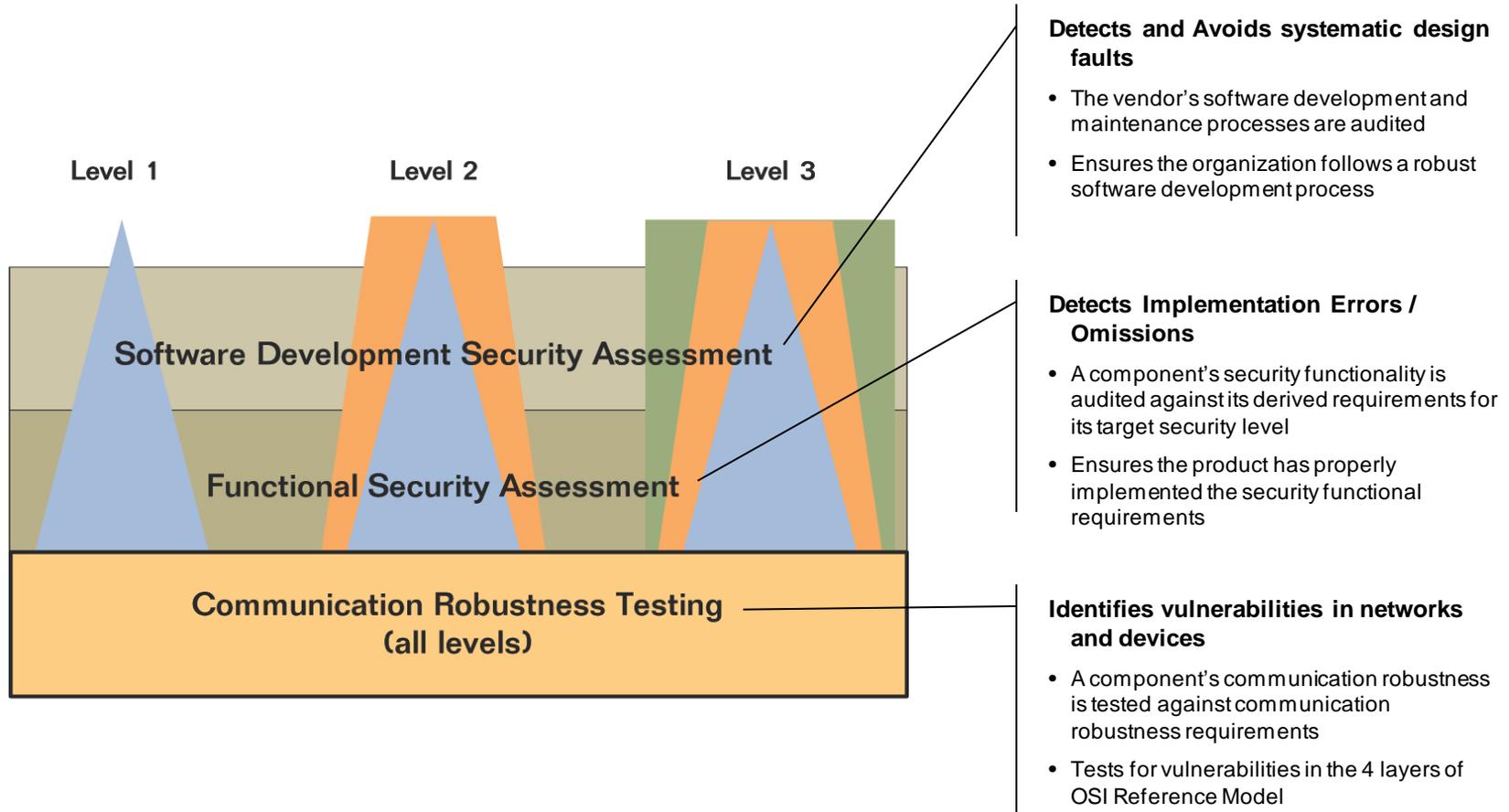
ISCI Program Outreach

- New website www.isasecure.org launched Q1 2010 – ongoing updates
- *ISASecure* EDSA Certification Specifications and Program Definition Documents Approved and posted for public access at www.isasecure.org
- ISCI Board donated EDSA FSA and SDSA technical specification to ISA-99 Committee via ISA99-ISCI Joint Working Group
- Webinar Series commencing in Q4 2010

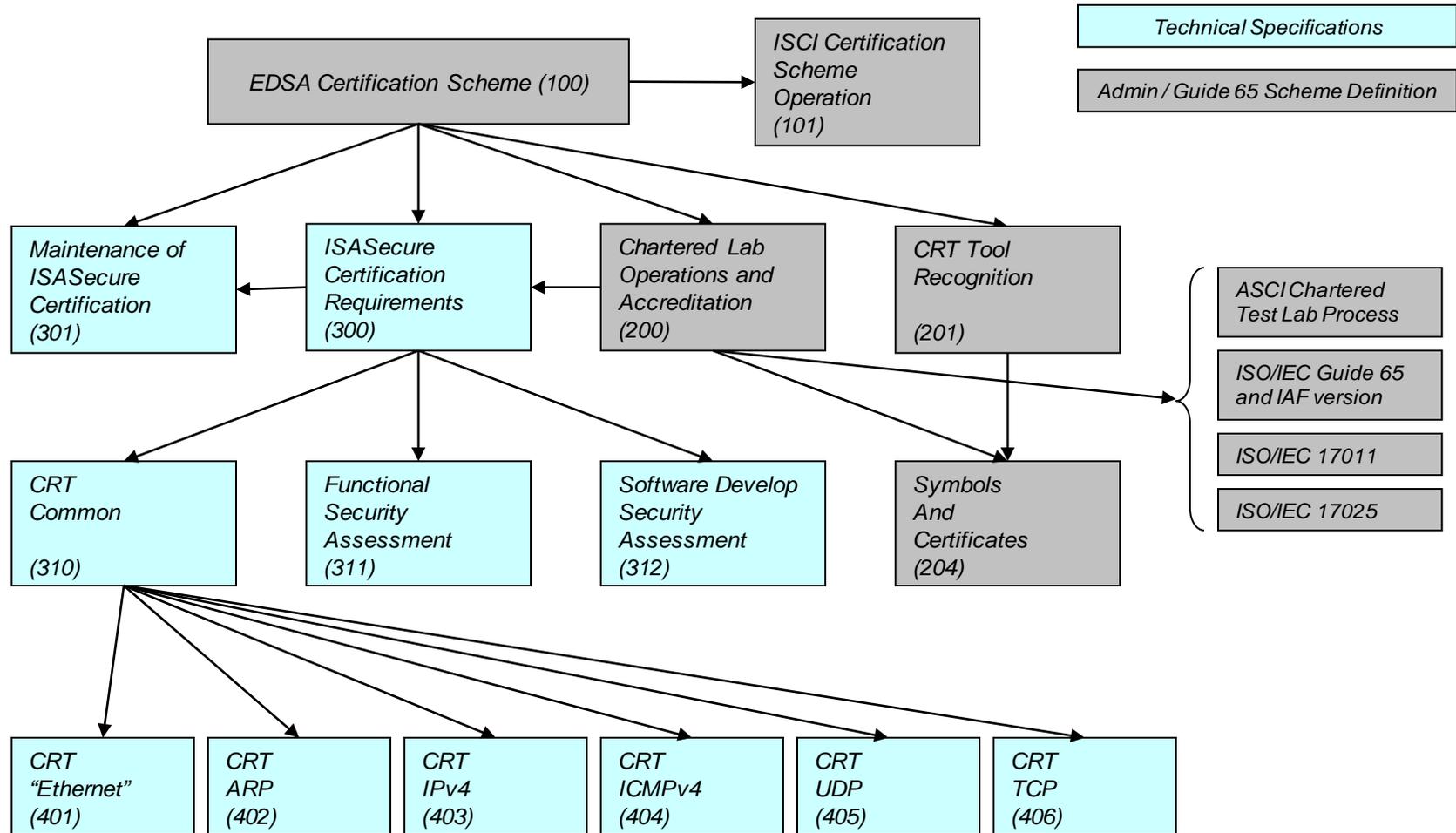


ISASecure Embedded Device Security Assurance (EDSA) Program

ISASecure EDSA Certification Levels



ISASecure EDSA Program Definition



Software Development Security Assessment (SDSA)

Secure Software Engineering

Purpose:

- Verification and validation that software for the device or system under test was developed following appropriate engineering practices to minimize software errors that could lead to security vulnerabilities.
- Not necessary to repeat the assessment if multiple products are developed by the same organization.

Composition

- Set of requirements, derived from existing reference standards and traceable to source standard (IEC 61508, ISO/IEC 15408)
- One or more acceptable arguments identified for each requirement

Software Development Security Assessment

- At all levels, the SDSA covers requirements for the following development lifecycle phases:
 - Security Management Process
 - Security Requirements Specification
 - Software Architecture Design
 - Security Risk Assessment and Threat Modeling
 - Detailed Software Design
 - Document Security Guidelines
 - Software Module Implementation & Verification
 - Security Integration Testing
 - Security Process Verification
 - Security Response Planning
 - Security Validation Testing
 - Security Response Execution

SDSA – Reference Standards

Reference Standards for Software Development Security Assessment		
[N4]	ISO/IEC 15408-1 through 15408-3	Information technology — Security techniques — Evaluation criteria for IT security — Part 1 through Part 3
[N6]	IEC 61508 Part 3	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software Development
[N7]	RTCA/DO-178B	Software Considerations in Airborne Systems and Equipment Certifications
[N8]	ISBN-13: 978-0735622142	The Security Development Lifecycle, M. Howard, S. Lipner, Microsoft Press (June 28, 2006)
[N9]	OWASP CLASP	OWASP CLASP (Comprehensive, Lightweight Application Security Process)

Functional Security Assessment (FSA)

Security Feature Tests

Purpose:

- Verification and validation that the device or system under test incorporates a minimum set of security features needed to prevent common security threats

Composition

- Set of requirements, derived from existing reference standards and traceable to source standard
- One or more acceptable solutions (countermeasures) identified for each requirement
- If applicable, procedures to verify the requirement has been satisfied

FSA – Reference Standards

[N1]	ISA-99.01.03D2-20090527	Security for Industrial Automation and Control Systems: System Security Requirements and Security Assurance Levels ISA-99.01.03
[N2]	NERC Standards CIP-001-1 through CIP-001-9	North American Electric Reliability Council Cyber Security Standards
[N3]	NIST 800-53	Recommended Security Controls for Federal Information Systems
[N4]	ISO/IEC 15408-1 through I5408-3	Information technology — Security techniques — Evaluation criteria for IT security — Part 1 through Part 3
[N5]	DHS Catalog	Department of Homeland Security: Catalog of Control Systems Security: Recommendations for Standards Developers

Communication Robustness Tests (CRT)

- Measures the extent to which network protocol implementations on an embedded device defends themselves and other device functions against unusual or intentionally malicious traffic received from the network.
- Inappropriate message response (s), or failure of the device to continue to adequately maintain essential services, demonstrates potential security vulnerabilities within the device.

CRT – Reference Sources

- ISO/IEC protocol standards and RFC's
- Centre for the Protection of National Infrastructure (CPNI)
 - Technical Note 3/2009 – Security Assessment of the Transmission Control Protocol (TCP)
- ISCI member vendor practices
- ISCI member asset owner protocol priorities
- Wurldtech Achilles Level 1 Test Specifications

ISCI / Wurldtech Collaboration

- Wurldtech has demonstrated a significant commitment to *ISASecure* EDSA Certification
 - Wurldtech collaborated with ISCI to merge Achilles Level 1 test specifications with *ISASecure* Communication Robustness Test (CRT) specifications.
 - Improved coverage gained from the combined specification
 - Wurldtech committed to provide *ISASecure* EDSA CRT test suites for ISCI via the Achilles product
 - *ISASecure* EDSA CRT test suites available to market in December 2010 Achilles product release
 - Wurldtech's Achilles Level 2 certifications *completed by accredited labs* will be recognized by ISCI towards an *ISASecure* certification

ISASecure EDSA Program Status

ISASecure EDSA Program will be operational in November, 2010

- *ISASecure* Embedded Device Security Assurance (EDSA) certification accepted as an ISO/IEC Guide 65 conformance scheme by ANSI/ACCLASS (<http://www.ansi.org/isasecure>)
- exida is the first *ISASecure* EDSA Chartered Test Lab to apply for the ANSI/ACCLASS ISO/IEC Guide 65 accreditation program for *ISASecure* EDSA Certifications
- Wurldtech Achilles Satellite test platform is the first CRT test tool to be submitted to ISCI for the ISO/IEC Guide 65 CRT Tool Recognition process
- First embedded controller from a major supplier submitted for *ISASecure* Certification with December 2010 target completion date



Who to contact for more information

Who to Contact to Certify Products

ISASecure EDSA Chartered Lab

exida

John Cusimano

Director of Security Services

Phone: (215) 453-1720

Fax: (215) 257-1657

Email: jcusimano@exida.com

Website: <http://www.exida.com>

Who to contact for CRT Test Tool

<http://www.wurldtech.com>

Wurldtech Security Technologies, Inc.

Greg Maciel

Achilles Sales Manager

Phone: (949) 300-4040

Email: gmaciel@wurldtech.com

Who to contact for ISCI Membership

Andre Ristaino

Managing Director, ASCI

Direct Phone: 919-990-9222

Fax: 919-549-8288

Email: aristaino@isa.org

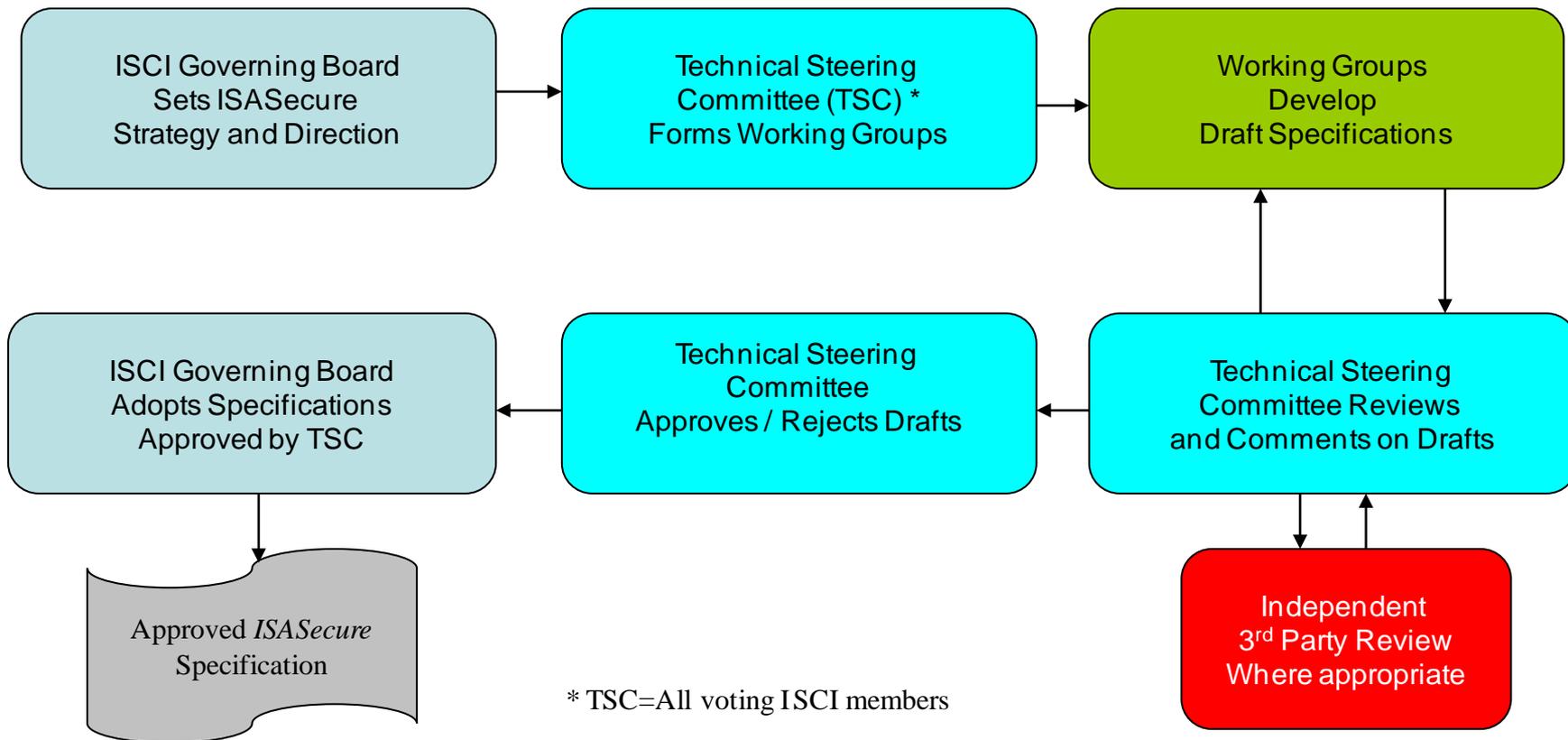
Website: <http://www.isasecure.org>



Reference material

ISASecure Specification Development Process

ISCI is used draft ISA99 Derived Requirements framework as a basis for organizing *ISASecure* test specifications.



ISA 99 Work Products

