



**IEC 62443-2-4:
A Baseline Security Standard for
Industrial Automation Control Systems**

History Part I

The WIB – A Collection of End Users

The Werkgroep Instrument Beoorderling (WIB), or the international instrument users association

Comprised of over 50 end-users from various industrial sectors located around the world

Collaborate to solve various manufacturing challenges

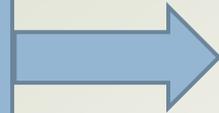
History

- Founded In 1962 (The Netherlands)
- 75+ Global End-user Members
- Plant Security Sub-working Group led by Shell cyber security team



The WIB Storyline: From Concept To Standard

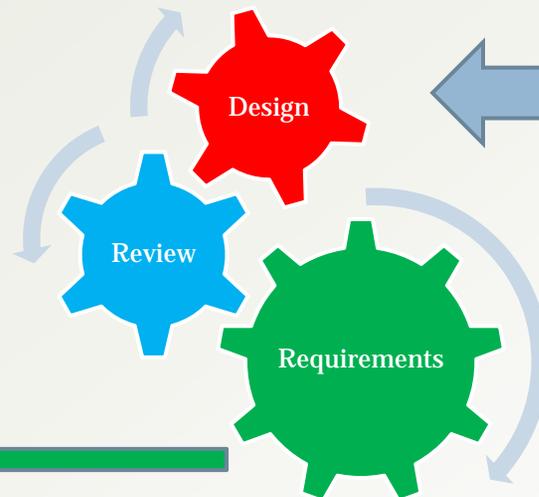
NERC/CIP, CFATS,
DHS Procurement
Language, ISAPS99,
NIST 800-53, ISO
2700x, NIST IR 7628
etc, etc, etc.



Select the low
hanging fruit



First industry driven standard



The WIB security requirements

The WIB Plant Security Working Group (PSWG) announced version 2 of the security requirements for Vendor's in November 2010

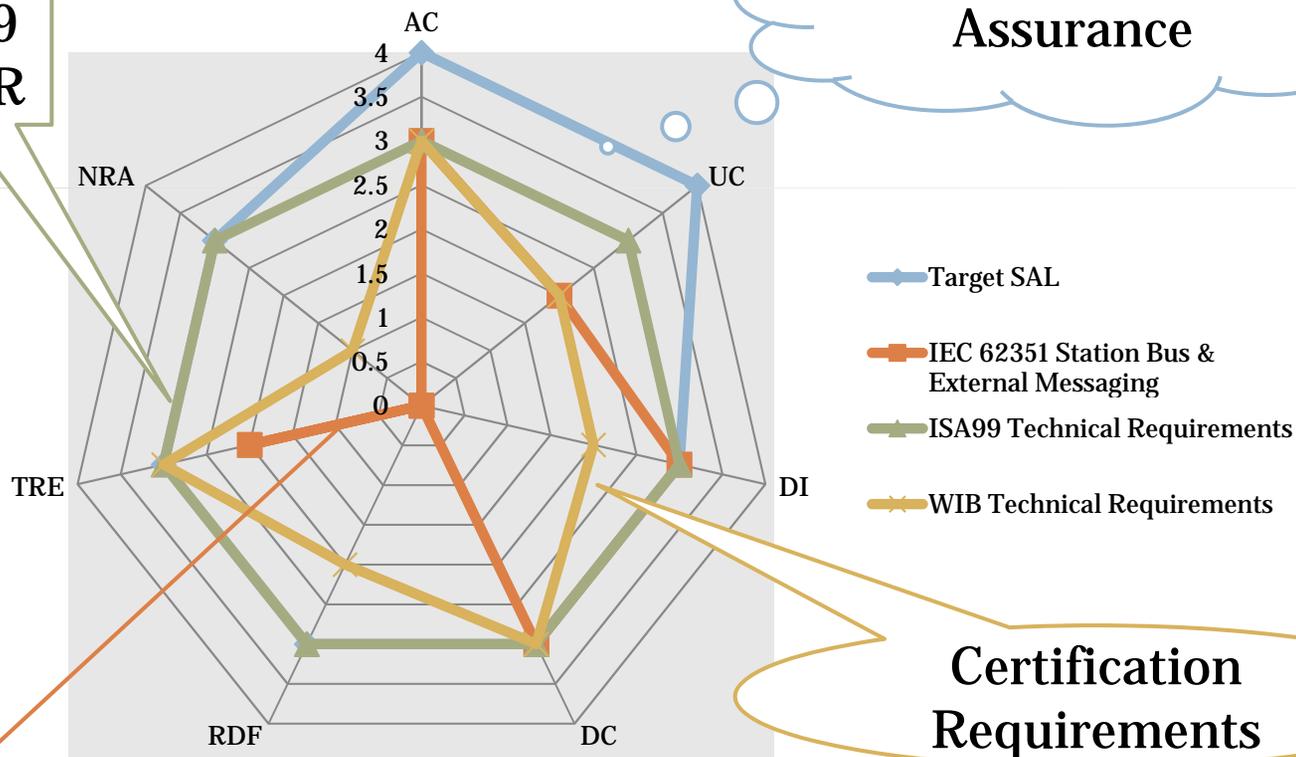
- 2 versions with 4 revisions
- 50+ stakeholders: *vendors, end-users, consultants, subject matter experts*
- Over 1000 comments/change requests
- Aligned To IEC framework for future adoption (IEC 62443-2-4 approval pending)



Comparison of security assurance

ISA99
FR/SR

Objective Security Assurance



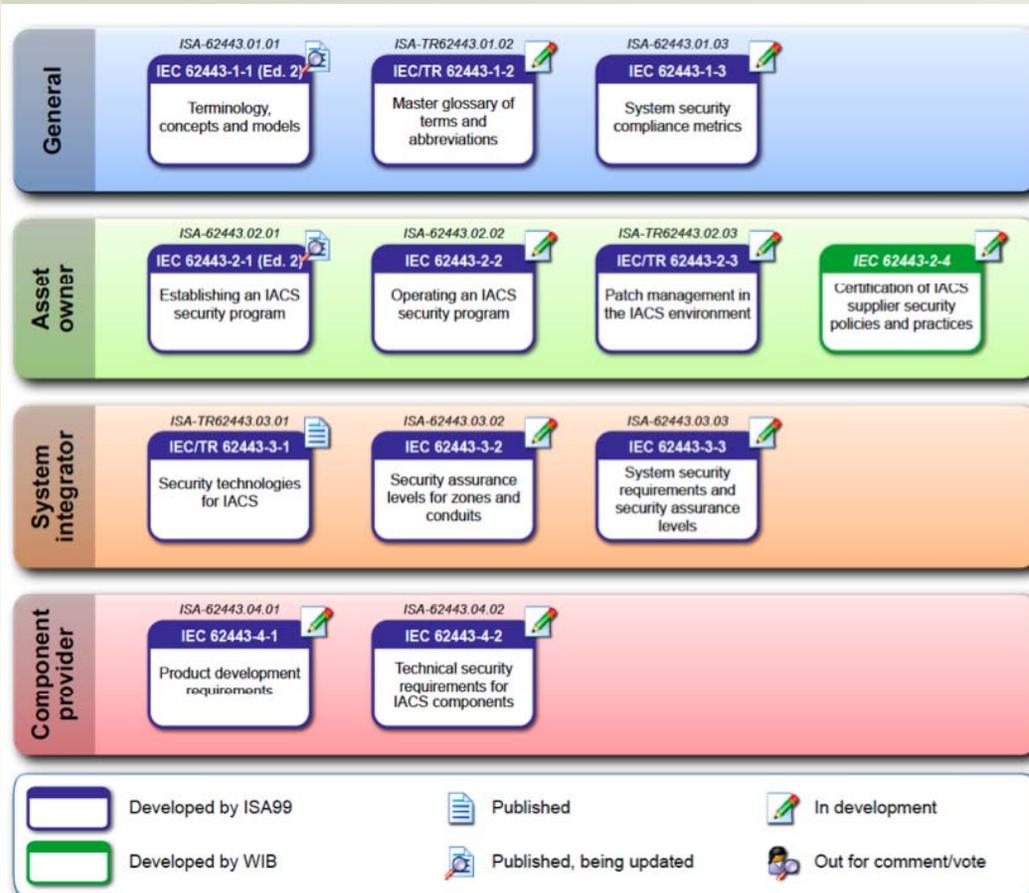
Certification Requirements

- IEC62531
- IEC Parent Systems

FR – Foundational Requirements
SR – System Requirements

History Part II

Alignment with ISA99 & NISTIR 7628



65/482/NP

NEW WORK ITEM PROPOSAL

Proposer NL	Date of proposal 2011-04-13
TC/SC 65	Secretariat FR
Date of circulation 2011-04-15	Closing date for voting 2011-07-15

A proposal for a new work item within the scope of an existing technical committee or subcommittee shall be submitted to the Central Office. The proposal will be distributed to the P-members of the technical committee or subcommittee for voting on the introduction of it into the work programme, and to the O-members for information. The proposer may be a National Committee of the IEC, the secretariat itself, another technical committee or subcommittee, an organization in liaison, the Standardization Management Board or one of the advisory committees, or the General Secretary. Guidelines for proposing and justifying a new work item are given in ISO/IEC Directives, Part 1, Annex C (see extract overleaf). **This form is not to be used for amendments or revisions to existing publications.**

The proposal (to be completed by the proposer)

Title of proposal
Security for industrial process measurement and control – Network and system security
Part 2-4: Certification of IACS supplier security policies and practices

Standard Technical Specification

Scope (as defined in ISO/IEC Directives, Part 2, 6.2.1)
Part 2-4 specifies security certification requirements in four categories: organizational, system capabilities, system acceptance testing and commissioning, and maintenance and support. These requirements are prescriptive and measurable to ensure that the evidence submitted by vendors applying for certification for the certifying a

Purpose and justify
Environmental aspects
1) Standardize an effort by major
2) Harmonize the

Target date
Estimated number of n post-NP+CD, post-C

Proposed working draft
Relevant documents
Align this part (Pa preparation

Relationship of proje ISO/IEC JTCl/SC:

Liaison organization:

Preparatory work
Ensure that all copyrig
 A draft is i
* Recipients of this do they are aware and t We nominate a projec mail): Dennis Holste

WIB 2.0 – NISTIR 7628 Alignment

Principal Investigators:
William F. Rush
Dennis K. Holstein

This paper summarizes OCG's analysis and assessment of the alignment between WIB 2.0 and NISTIR 7628. OCG concludes these documents show a high degree of alignment, given their different audiences and industry of origin. In fact, there are no conflicts. There are areas which should be improved in the WIB report, which are under consideration for the next release – WIB 3.0.

OPUS Consulting Group
628 Island View Drive
Seal Beach, CA 90740
+1 562 715 4174
+1 562 430 1538 (fax)
6281@opus.com

APC and ISASecure

- APC (Achilles Practices Certification) is the certification program currently in place to assess conformity with the WIB requirements, which focuses on vendor security practices. It is currently managed by Wurltdtech Security Technologies, under approval from the WIB.
- ISASecure is the certification program managed by the ISA Security Compliance Institute to assess conformity with selected parts of the ISA99 Standards Roadmap. The first ISASecure product is the Embedded Device Security Assurance (EDSA) Certification, which focuses on device security characteristics.
- Both programs are complementary to each other.
- Both programs are continual works in progress.
- Both programs serve the security needs of the community **TODAY**.



NIST Cyber Security Working Group (CSWG)

NIST
National Institute of
Standards and Technology

SGiP

NIST Smart Grid Collaboration Wiki
Smart Grid Interoperability Panel Site

[Home](#) [About SGiP](#) [Membership](#) [Working Groups](#) [Priority Action Plans](#) [Knowledge Center \(IKB\)](#) [News & Events](#) [Help/Contacts](#)

SmartGrid

Log In



Getting Started



Become A Member



TWiki Help



Member Resources



Upcoming Events



Catalog Standards



SGIP Brochures

TWiki > SmartGrid

Web > [SGiPWorkingGroupsAndCommittees](#) > [CyberSecurityCTG](#) > [CSCTGHighLevelRequirements](#) > [IEC6244324TaskForce](#)
(2011-10-06, FrancesCleveland)

[Edit](#) [Attach](#)

This is the workspace for the IEC 62443-2-4 Task Force

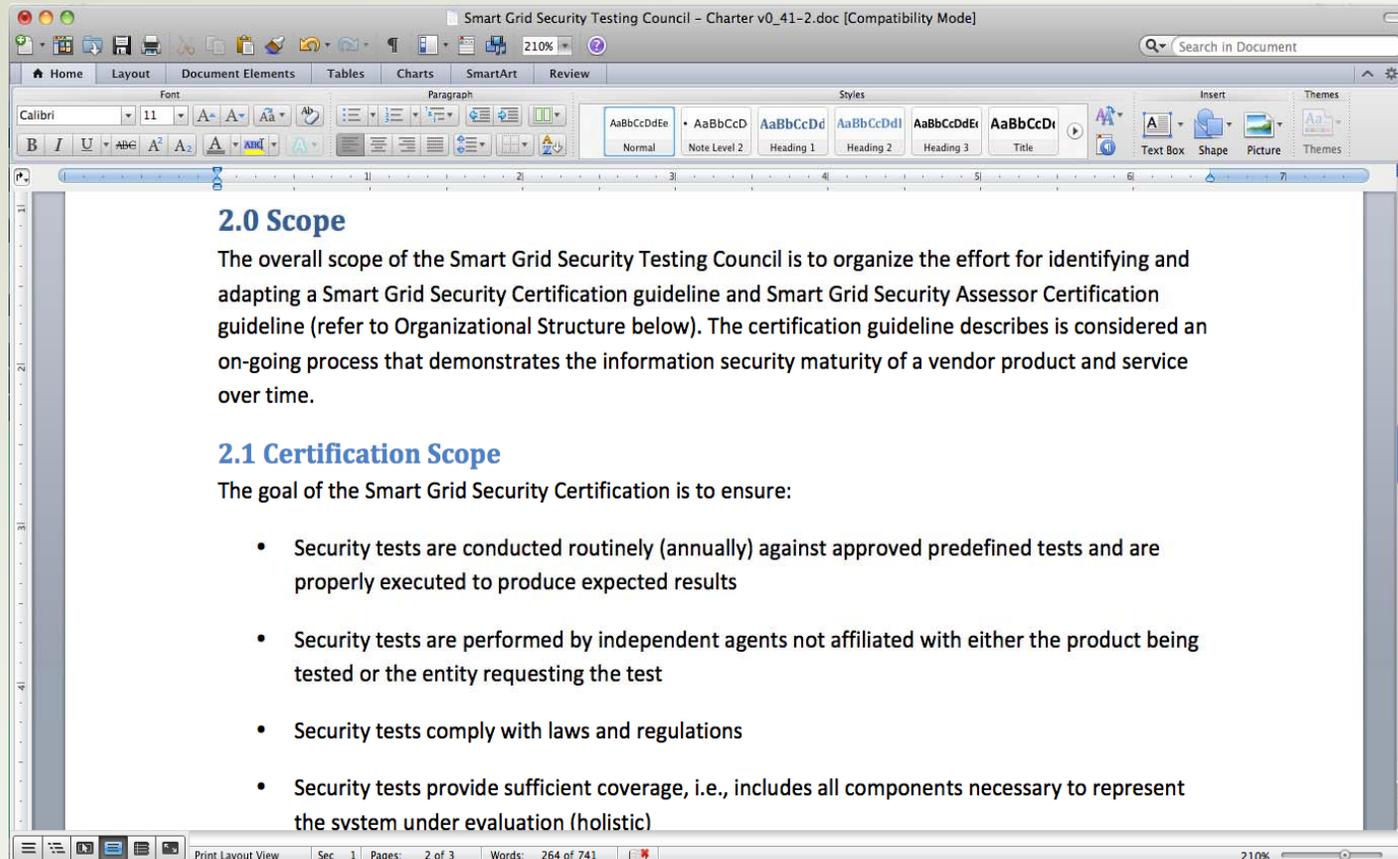
- Lead: Mike Ahmadi (mike.ahmadi@granitekey.com)
- The Group Mailing List address for the Task Force is the same as the HLR mailing list address: csctgrqmts@nist.gov (email marianne.swanson@nist.gov and tanya.brewer@nist.gov to be added to the group)
- Meeting Info: Fridays, 4-5 PM Eastern
- Dial In: 1-800-728-9607 (Toll Free), 1-917-904-9873 (Direct), Participant Passcode: 4570752
- The collaborative Google Doc is available by following this link:
https://docs.google.com/document/d/1v3MYYx_ZXp9MozolYwxcNu3jmDhCNZ98V2W8crXknU4/edit?hl=en_US&authkey=C1fEq84H# . Please put your name in the Attribute column and add your comments. Do not alter anyone else's comment **[THE COMMENT PERIOD FOR THIS DOCUMENT IS CLOSED]**
- Due to potential copyright issues, we will not host any IEC 62443 series documents on this site. Please contact Tom Phinney at tom.phinney@cox.net and he will provide you with the relevant IEC draft documents.

To join, please contact Tanya Brewer (tanya.brewer@nist.gov).

- [WIB 2.0 - NISTIR 7628 Alignment 2011-03-16.pdf](#): WIB 2.0 and NISTIR 7628 Alignment Document
- [WIB 2.0 - NISTIR 7628 Alignment 2011-03-16.pdf](#): WIB 2.0 and NISTIR 7628 Alignment Document

UCAIug OpenSG Security Conformity Task Force

- Task force formed under OpenSG to address security conformity
- Could serve as adjudicator for member organizations



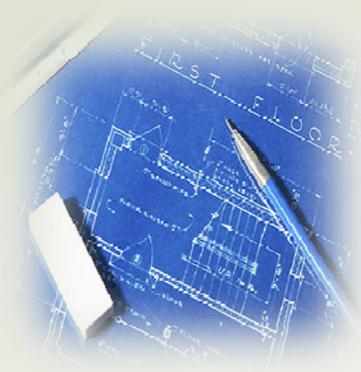
Enormous Outpouring of Participation In IEC Project

- Over 50 participating organizations from public, private, and academic sectors
- Participation from major countries (including US, China, Japan, Holland, France, Switzerland, Germany, Brazil...and many more)
- Over 1000 comments



From Requirements To Vendor Certification

- Build on WIB 2.0
- Blessed by PSWG



- Over a year of pilot programs
- Multiple vendors
- Various industry sectors

- Scalable certification program
- Internationally accepted frameworks
- Formal, testable criteria



- WIB accredited November 2010
- 1st certified vendor January 2011



Scalability: the certification levels



Bronze certification: 148 of 272 Requirements

Entry-level certification, awarded for successful completion of all applicable requirements for security policies and practices that have been implemented and verified through direct measurement or analysis.



Silver certification: 218 of 272 Requirements

Awarded for successful completion of all applicable requirements and selected requirement enhancements that have been implemented and verified through direct measurement or analysis.



Gold certification: 272 of 272 Requirements

Awarded for successful completion of all applicable security policies and practices that exist in a vendor's system. Gold level contains additional performance and industry-specific requirements.

The requirements framework

Organization

System Capability

System Testing & Commissioning

Maintenance & Support

Process Area Categories	Process Area ID	Process Area Subject
Organizational Process Areas	PA01	Prepare & Inform Personnel
	PA02	Designate a Security Contact
	PA03	Specify Base Practices
System Capability Process Areas	PA04	Harden the System
	PA05	Protect from Malicious Code
	PA06	Implement Patch Management
	PA07	Secure Account Management
	PA08	Support Backup/Restore
	PA09	Increase Network Visibility
	PA10	Standardize Historical Interfaces
	PA11	Verify Operations
	PA12	Connect wirelessly
	PA13	Priority security instrumented system (PUS) Connectivity
	PA14	Provide Remote Access
	PA15	Protect Data
System Acceptance Testing & Commissioning Process Areas	PA16	Manage the Deployment
	PA17	Harden the System
	PA18	Protect from Malicious Code
	PA19	Implement Patch Management
	PA20	Secure Account Management
	PA21	Support Backup/Restore
	PA22	Implement the Architecture
	PA23	Connect wirelessly
	PA24	Provide Remote Access
	PA25	Protect Data
Maintenance & Support Process Areas	PA26	Manage the Deployment
	PA27	Harden the System
	PA28	Protect from Malicious Code
	PA29	Implement Patch Management
	PA30	Secure Account Management
	PA31	Support Backup/Restore
	PA32	Implement the Architecture
	PA33	Connect Wirelessly
	PA34	Provide Remote Access
	PA35	Protect Data

■	PA01: Prepare and Inform Personnel	BP.01.01: Requirement recognition and enforcement	BR: The Vendor shall ensure that personnel within its organization, subcontractors, and consultants who are assigned to activities of the Principal have been informed that the Vendor Base Practices (this document) contains mandatory requirements for all services or deliverables to the Principal. Note: Terms and Conditions (T&C) for subcontractor and consultant contracts and purchase orders should include a requirement to adhere to the WIB standards and practices.	Bronze
■			RE(1): Vendor representatives shall enforce the control system security procedures specified in this document and the Vendor's applicable security policies during engagement in activities on the Principal's site.	Silver
■			RE(2): The Vendor shall have policies and procedures to support an incident response team led by the Principal.	Silver
■			RE(3): The Vendor shall ensure that personnel within its organization, subcontractors, and consultants acknowledge and comply with security policies enforced by the Principal.	Gold

Organizational process area

- Category Description: Requirements and Enhancements targeted at organization policies and procedures
- Conformance Criteria: Proof of policy existence and evidence of its application

■		BP.06.02: Patch qualification	<p>BR: The Vendor shall qualify all relevant software patches and service packs for use on its system during its supported lifetime including security patches that are released by the manufacturer of the operating system and third party software used on their system.</p> <p>Note: Patch testing and qualification, and more importantly deploying necessary patches should follow the guidelines offered in ISA-99.02.03.</p>	Bronze
■			<p>RE(1): If a security patch is considered not relevant by the Vendor for use on its system, the reason shall be provided to the Principal.</p>	Bronze
■			<p>RE(2): If a security patch is not approved by the Vendor for use on its system, then the reason and remediation plan shall be provided to the Principal. The remediation plan shall describe how a solution will be provided within 12 months.</p>	Bronze

System capability process area

- **Category Description:** Requirements and enhancements for security functions to be designed into the Vendor's system and compensating security functions used to protect Vendor's system components and subsystems which do not have built-in security capabilities
- **Conformance Criteria:** Proof of system capability and verification of functionality

■	PA19: Implement Patch Management	BP.19.01: Up-to-date systems	BR: For systems maintained by the Vendor, the Vendor shall keep the security patch levels of all ASD systems current to within 3 months of the security patch being available and qualified by the respective system Vendor.	Bronze
■			RE(1): If the installation of patches requires an outage that can impact operations or impacts performance, the Vendor shall develop and document a mitigation plan subject to approval by the Principal.	Bronze
■			RE(2): Vendor approved patches shall be approved by the Principal before they are installed on the Vendor's system.	Bronze

System testing and commissioning process area

- **Category Description:** Requirements and enhancements for demonstrating correct implementation of security functions built into the vendor's system, and readiness of system turnover for operation by the Principal or his selected Operator
- **Conformance Criteria:** Verification of security functionality and existence of operational polices

■	PA28: Protect from Malicious Code	BP.28.01: General anti-virus policy	BR: Prior to scheduled maintenance, the Vendor shall update the document describing the configuration of the virus detection software installed on each ASD component.	Bronze
■		BP.28.02: Portable media procedure	BR: Prior to schedule maintenance the Vendor shall update documents describing changes to a procedure for its staff stating that portable media (e.g. laptops and USB storage) used by the Vendor for commissioning and maintenance of equipment or devices in the ASD are used for this purpose only.	Bronze
■		BP.28.03: Anti-virus management	BR: Prior to scheduled maintenance, the Principal shall document changes to the installation of virus definition files have been installed and verified within 30 days after being qualified by the system Vendor.	Bronze

Maintenance & support process area

- **Category Description:** Requirements and Enhancements for demonstrating correct maintenance of security functions built into the Vendor's system, and timely support in response to security related events
- **Conformance Criteria:** Existence of policy and its application and verification of functionality.

The Certification Process

Phase 1

Scoping – the key to success

Certification scope and planning

Define applicable requirements & exceptions

Phase 2

Preparation – vendor heavy lifting

Vendor self-appraisal, collecting evidence & warrants,

Assessor quick review

Phase 3

Appraisal – scoring the evidence

Vendor submits final data

Assessor review & request evidence and clarification

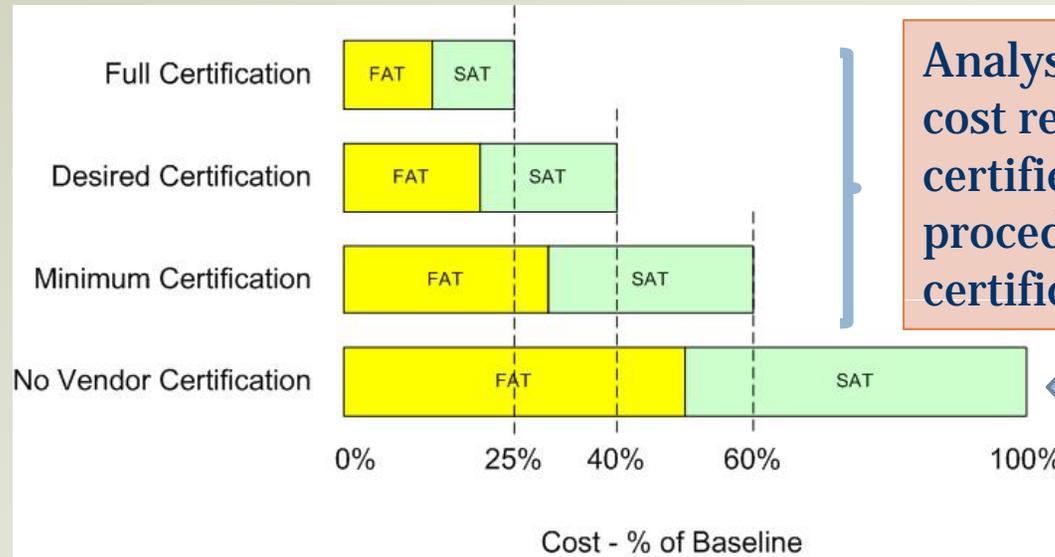
Phase 4

Reporting – the finish line

Collate findings, observations and recommendation

Certificate issue.

The cost of certification is recoverable



Analysis shows the reduction in cost realized if Vendor is security certified 40%-75%; test plans, procedures are in place to satisfy certification

- Successfully completing FAT & SAT is required to deploy, operate and maintain the process control system
- Given the requirements to operate securely, security testing must be an integral part of FAT & SAT

Vendor not certified must develop and exercise proper security test plans and procedures – this cost is well defined