WST FUNCTIONAL CYBER SECURITY FOR CRITICAL INFRASTRUCTURES

Functional Cyber Security Requirements For Vendors

The First International Cyber Security Standard For Global Process Automation & Control System Vendors

Presented By:

Tyler Williams, Wurldtech

Peter Kwaspen, Shell Oil

Presentation Purpose

To introduce the WIB Process Control Domain – Security Requirements For Vendors Standard and associated Achilles Practices Certification program, it's purpose, structure, benefits and overall business case, to the ICSJWG attendees.

Agenda

Section 1 – Background & Catalysts

Section 2 – The WIB Standard & Certification Program

Section 3 – The Path To Success For Stakeholders

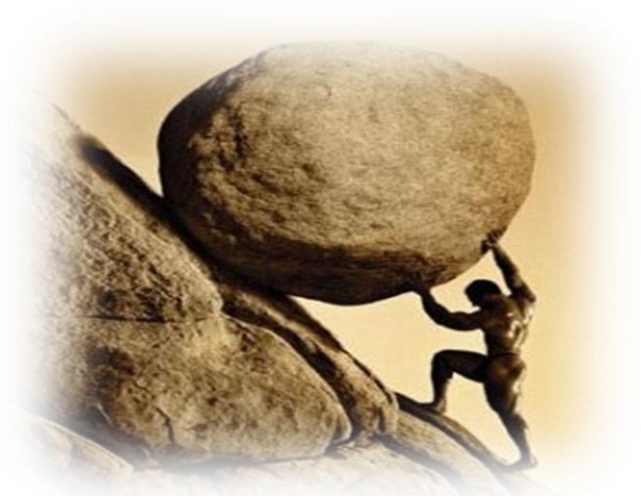
First Things First…

- Let's All Get Aligned
- "Don't Let The Perfect Be The Enemy Of The Good"
- Lets Try Something New…

The Landscape Until Now…

- Too Much FUD, Not Enough Facts
- No Common Language Or Communications Framework
- Asymmetric Stakeholder Efforts “Workinggroupitis”
- No Data, No Business Case, No Budget, No Improvement
- Unclear / Undefined Stakeholder Roles & Ownership
- Suboptimal Internal / External Economic Conditions
- Product Pitches Instead Of Functional Solutions
- Led To….

ICSJWG 2010 Spring Conference Presentation



Common Cyber Security Benchmarks

Achilles Certified
Industrial Devices, Systems & Applications

Achilles Certified
Cyber Security Best Practices

Achilles Certified
Industrial Automation Professionals

Section 2: Practices Certification

1. The History
2. The Rules
3. The Benchmark
4. The Reference Model
5. The Framework
6. The Requirements
7. The Evidence
8. The Process
9. The Result

The History

Phase 1 – Finalize WIB Requirements

Phase 2 – Make Requirements Generic For Wide Adoption

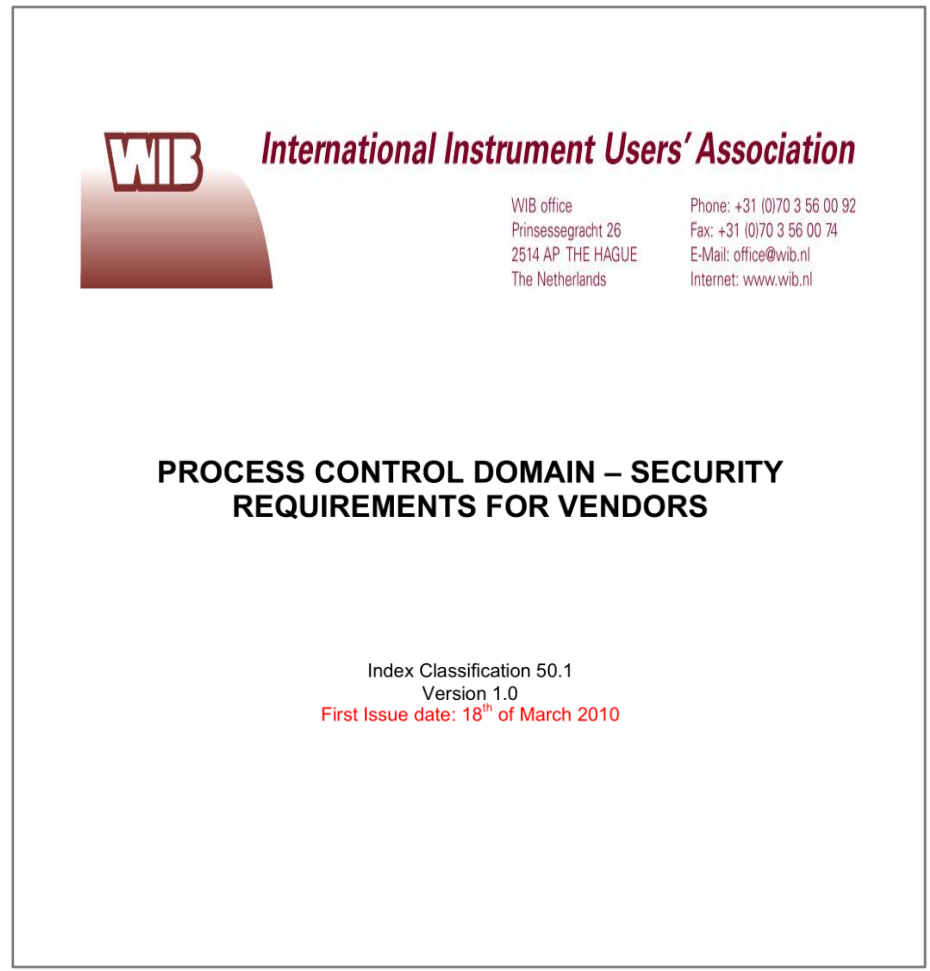
Phase 3 – Create A Certification Program Framework

Phase 4 – Pilot The Program & Launch

The Rules

- Purpose Driven
- Functional
- Open
- Scalable
- Repeatable
- Cost Effective
- Simple
- Defensible

The Benchmark



International Instrument Users' Association

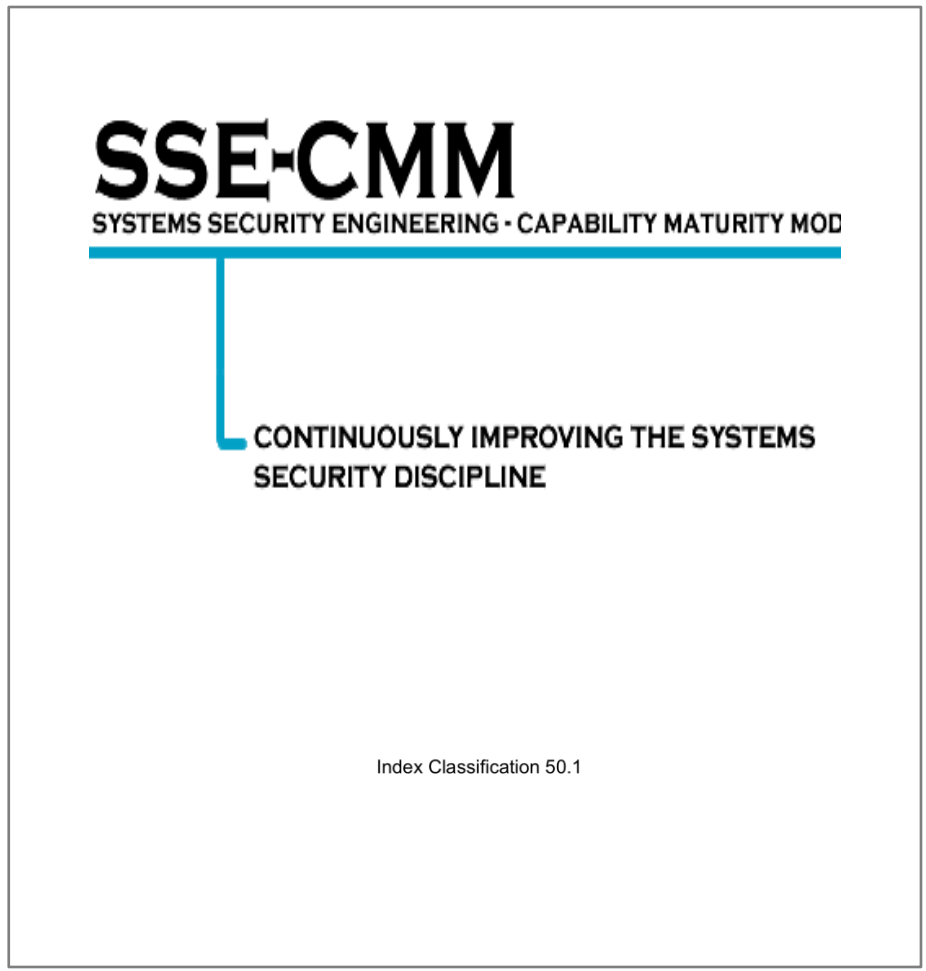
WIB office
Prinsessegracht 26
2514 AP THE HAGUE
The Netherlands

Phone: +31 (0)70 3 56 00 92
Fax: +31 (0)70 3 56 00 74
E-Mail: office@wib.nl
Internet: www.wib.nl

PROCESS CONTROL DOMAIN – SECURITY REQUIREMENTS FOR VENDORS

Index Classification 50.1
Version 1.0
First Issue date: 18th of March 2010

The Reference Model



The SSE-CMM has two dimensions, “domain” and “capability.” The domain dimension simply consists of all the practices that collectively define security engineering. These practices are called “base practices.” The capability dimension represents practices that indicate process management and institutionalization capability.

The Framework

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
Product 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 on Historians
	PA11	Control Set Points
	PA12	Connect Wirelessly
	PA13	Fortify Safety Instrumented System (SIS) Connectivity
	PA14	Provide Remote Access
Commissioning & Maintenance Process Areas	PA15	Manage the Deployment
	PA16	Harden the System
	PA17	Protect from Malicious Code
	PA18	Implement Patch Management
	PA19	Secure Account Management
	PA20	Support Backup/Restore
	PA21	Implement the Architecture
	PA22	Connect Wirelessly
	PA23	Provide Remote Access

Wurldtech has tailored twenty three (23) Process Areas to be used by Vendors applicants. These PAs are organized into three logical categories: (1) Organization Process Level, (2) Product Process rea, and (3) Commissioning & Maintenance Process Area. Table 1 describes the Process Area within each category.

The Requirements

Process Area Categories	PA	BP ID	Base Practice Objective
Organization Process Areas	PA01: Prepare and Inform Personnel	BP.01.01	Requirement recognition and enforcement
		BP.01.02	Ensure alignment
		BP.01.03	Protect sensitive documentation
		BP.01.04	Background checks
		BP.01.05	Competent personnel
		BP.01.06	Confidentiality and user agreements
	PA02: Designate a Security Contact	BP.02.01	Nominate the role
	PA03: Specify Base Practices	BP.03.01	Standards employed
		BP.03.02	Security certificates

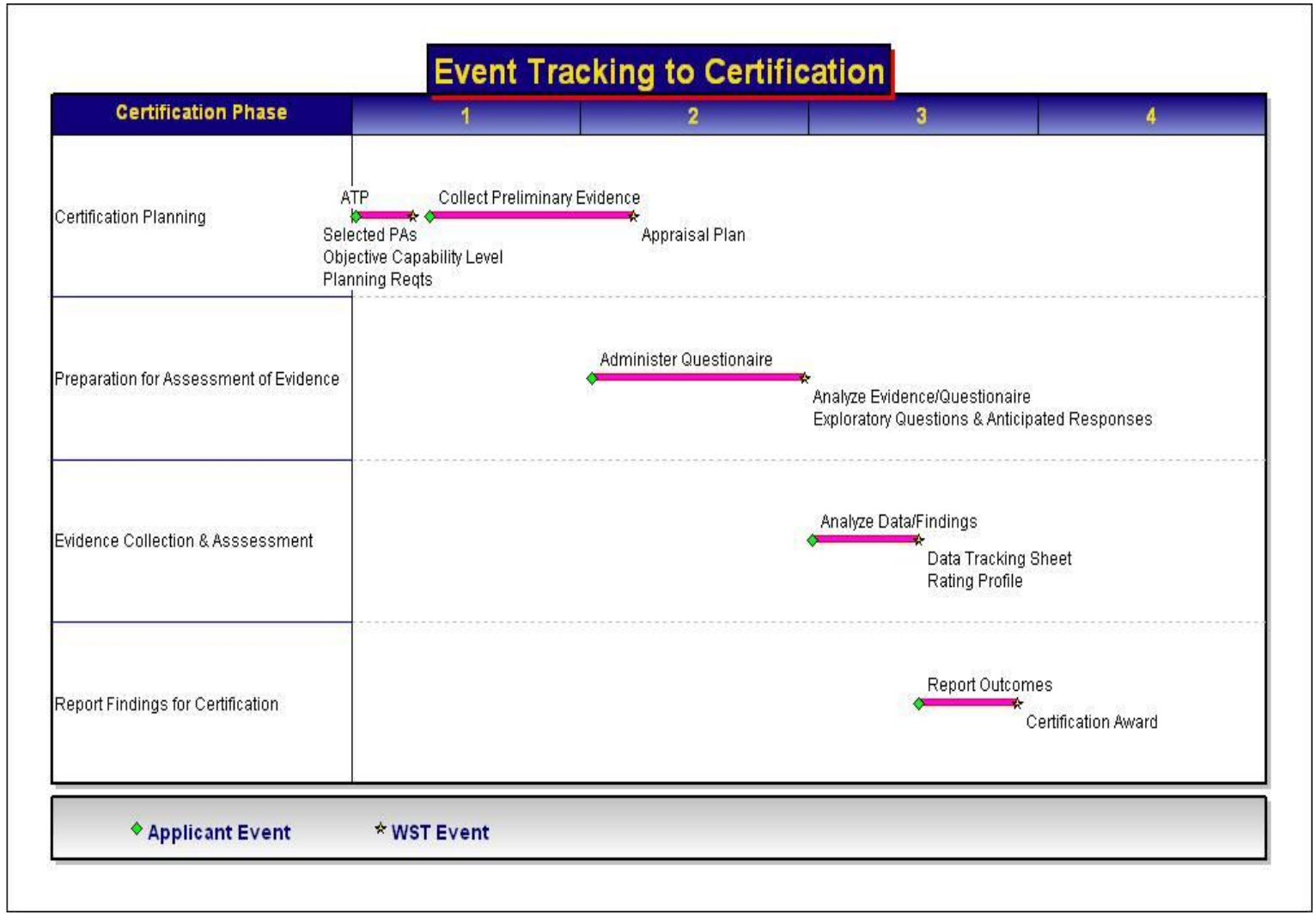
The Requirements

PA02: Designate a Security Contact	BP.02.01: Nominate the role	BR: The Vendor shall nominate a Process Control Security Focal Point in its organization who is responsible and accountable for the following activities. a. Acting as liaison with the Principal, as appropriate, about compliance of the Vendor's system with the Vendor APC Base Practices (this document). b. Communicating the Vendor's point-of-view on process control security to the Principal's staff. c. Ensuring that tenders to the Principal are aligned and in compliance with both the Vendors APC Base Practices (this document) and the Vendor's internal requirements for process control security. d. Communicating deviations from, or other issues not conforming with, the Vendors APC Base Practices (this document) to the Principal's organization requesting the tender. e. RE(1): Providing the Principal with timely information about cyber security vulnerabilities in the Vendor's supplied systems and services. f. RE(2): Providing timely support and advice to the Principal in the event of cyber security incidents involving the Vendor's systems or services.

The Evidence

Applicant's Response						Requirement Traceability				
QR #	Question Response			Evidence	Remarks	MRE ID	MRE #	Evidence Requirement	M	O
	YES	NO	Don't Know							
017						BP.02.01BR	017	Vendor senior manager signed affidavit which includes the signature of the Process Control Security Focal Point designee who has accepted responsibility for the activities specified in BP.02.01.	X	

The Process


Event Tracking to Certification
Certification Phase
1
2
3
4
Certification Planning
ATP
Collect Preliminary Evidence
Selected PAs
Objective Capability Level
Planning Reqts
Appraisal Plan
Preparation for Assessment of Evidence
Administer Questionaire
Analyze Evidence/Questionaire
Exploratory Questions & Anticipated Responses
Evidence Collection & Asssessment
Analyze Data/Findings
Data Tracking Sheet
Rating Profile
Report Findings for Certification
Report Outcomes
Certification Award
Applicant Event
WST Event

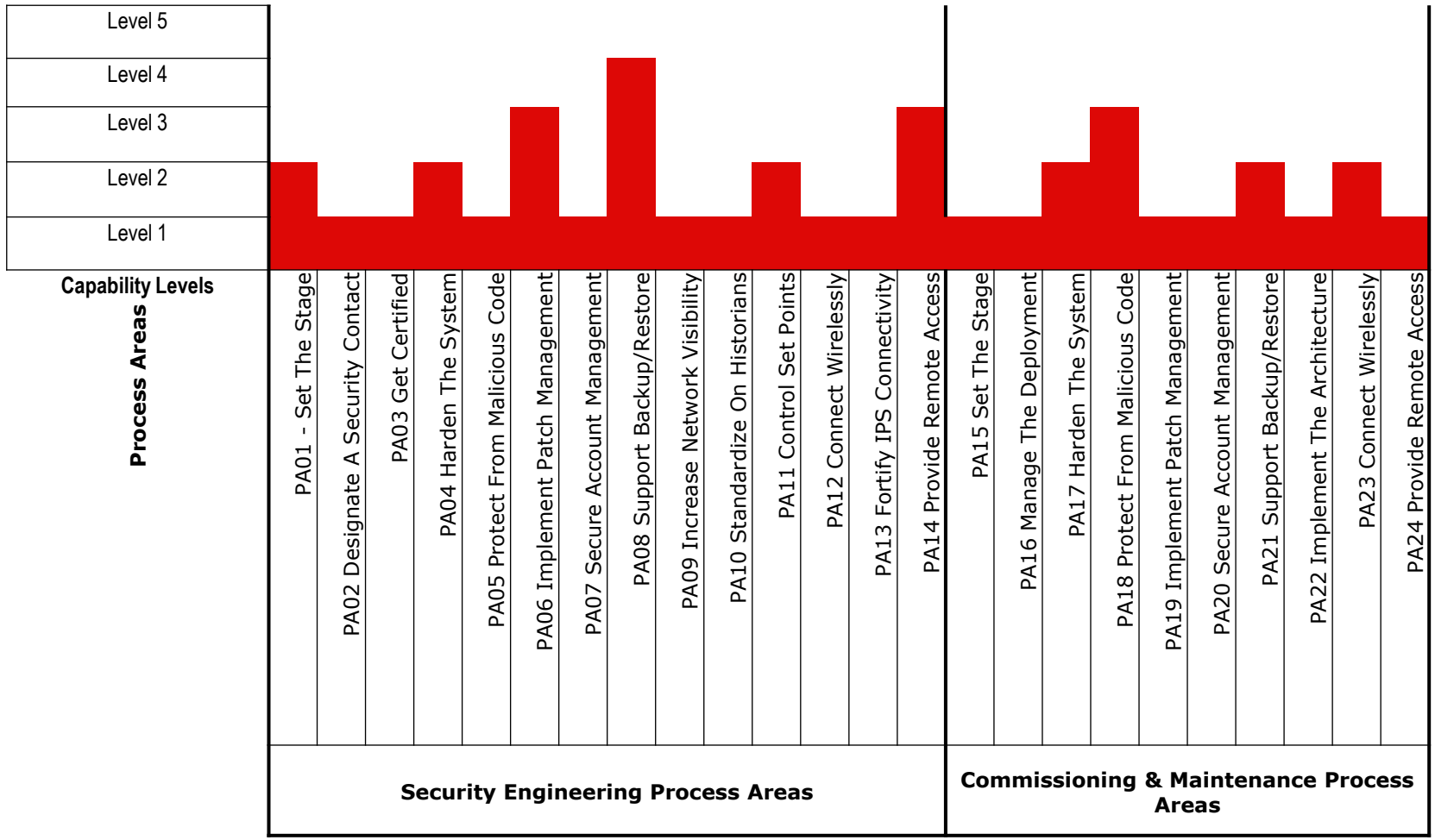
The Result

Bronze certification is awarded for successful completion of all applicable and approved Base Practices for Level 1 maturity.

Silver certification is awarded for successful completion of all applicable and approved Base Practices for Level 1 maturity and those Base Practices applicable to Level 2 maturity.

Gold certification is awarded for successful completion of all applicable and approved Base Practices for Level 1 maturity, those applicable to Level 2 maturity, and those applicable to Levels 3, 4 and 5 maturities.

The Result


Level 5
Level 4
Level 3
Level 2
Level 1
Capability Levels
Process Areas
PA01 - Set The Stage
PA02 Designate A Security Contact
PA03 Get Certified
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 On Historians
PA11 Control Set Points
PA12 Connect Wirelessly
PA13 Fortify IPS Connectivity
PA14 Provide Remote Access
PA15 Set The Stage
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
Security Engineering Process Areas
Commissioning & Maintenance Process Areas

The Status

HIMA

YOKOGAWA

INDUSTRIAL DEFENDER®

invensys

Brüel & Kjær

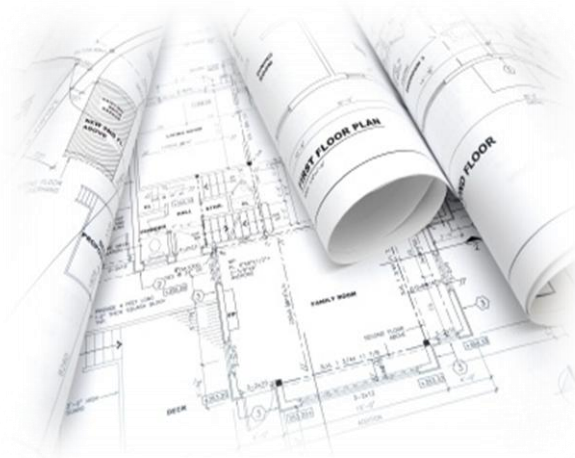
Pilot Program

- Five Global Suppliers
- Certified April 2010
- Finalize Practices Certification & Go To Market

Section 3: The Path To Success

Wurldtech

1. Lay The Foundation
2. Leverage Our Reputation To Drive Support
3. Increase Industry Stewardship



Vendors

1. Be Proactive & Get Involved

1. Use Security As A Differentiator

1. Align Internal Stakeholders

End Users

1. Stand On The Shoulders Of Giants
2. Insist On Product / Practice Certifications
3. Reward Vendor Leadership

Governments

1. Facilitate Information Sharing

1. Create Incentive Programs

2. Build The Business Case

1. Limit Involvement

Let's Recap

- The Final Requirements Were Created, Reviewed & Revised By Industry Stakeholders From Different Sectors & Regions

- The Certification Program Structure Is Simple, Scalable, Functional & Cost Effective

- The Program Model Follows International Certification Guidelines & Aligns With Current & Emerging Cyber Security Standards (NIST, ISA SP99)

- The Program Integrates A Internationally Recognized Maturity Concept To Enable Industry/Segment/Vendor Analysis

Questions?

Wurldtech Security Technologies
Suite 1680 – 401 West Georgia Street
Vancouver BC Canada V6B 5A1

T 604 669 6674
F 604 669 2902
info@wurldtech.com