Automating the Compliance Process for Industrial Automation and Control Systems

Uduak J. Daniels CISSP, CISM
ICS Cybersecurity Specialist
Saudi Aramco

About the Presenter

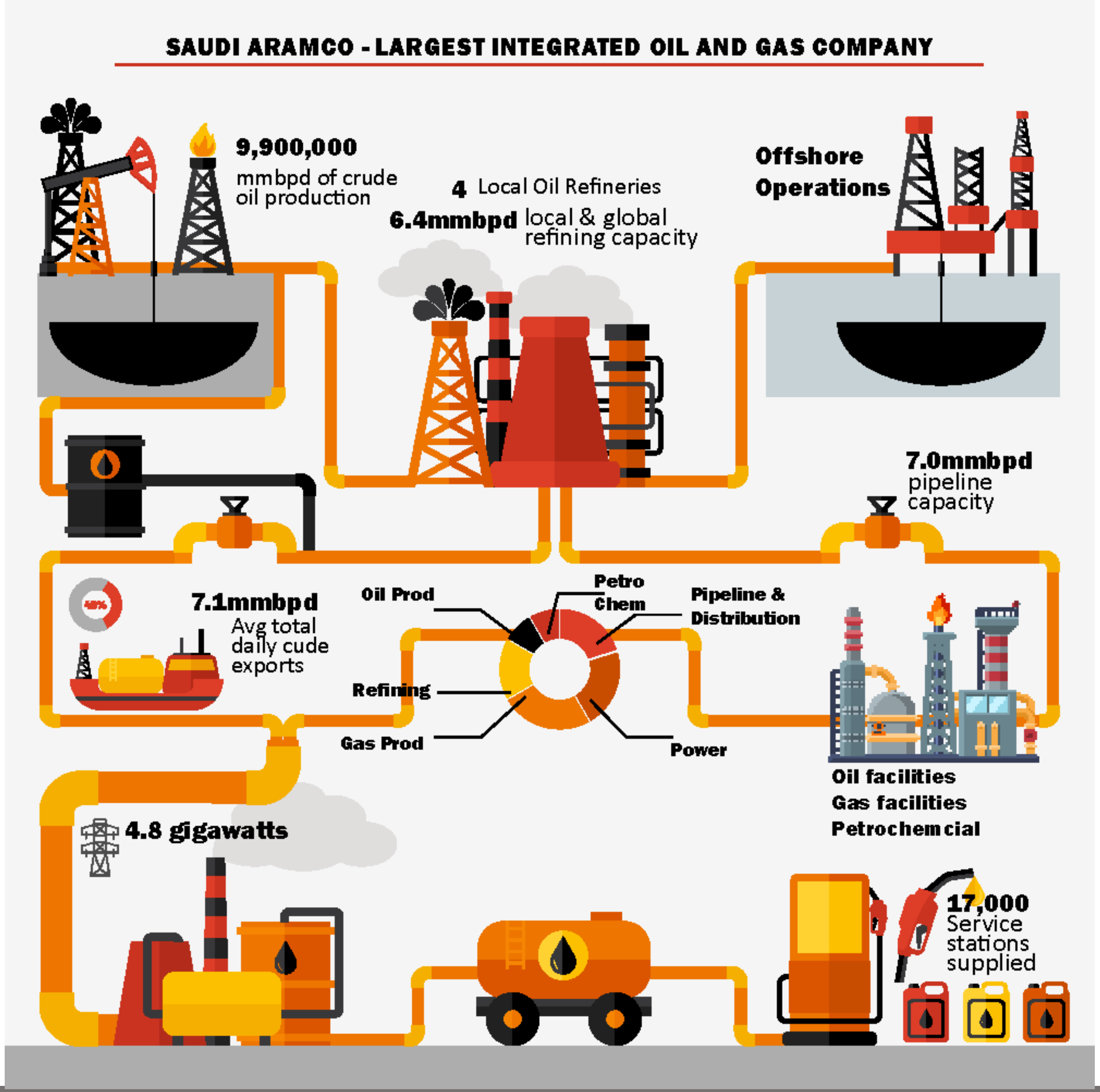
- Uduak Daniels
- 15 years experience in Cybersecurity
- 9 years Cybersecurity experience with asset owner
- CISSP, CISM
- VP ICS Cybersecurity Standards Committee Saudi Aramco
- Technical Steering Committee Member ISASecure

Presentation Overview

- Oil and Gas Operations
- IACS Cybersecurity Compliance
- Compliance Assessment
- Compliance Automation
- Compliance Assessment Tools

Oil and Gas Operations

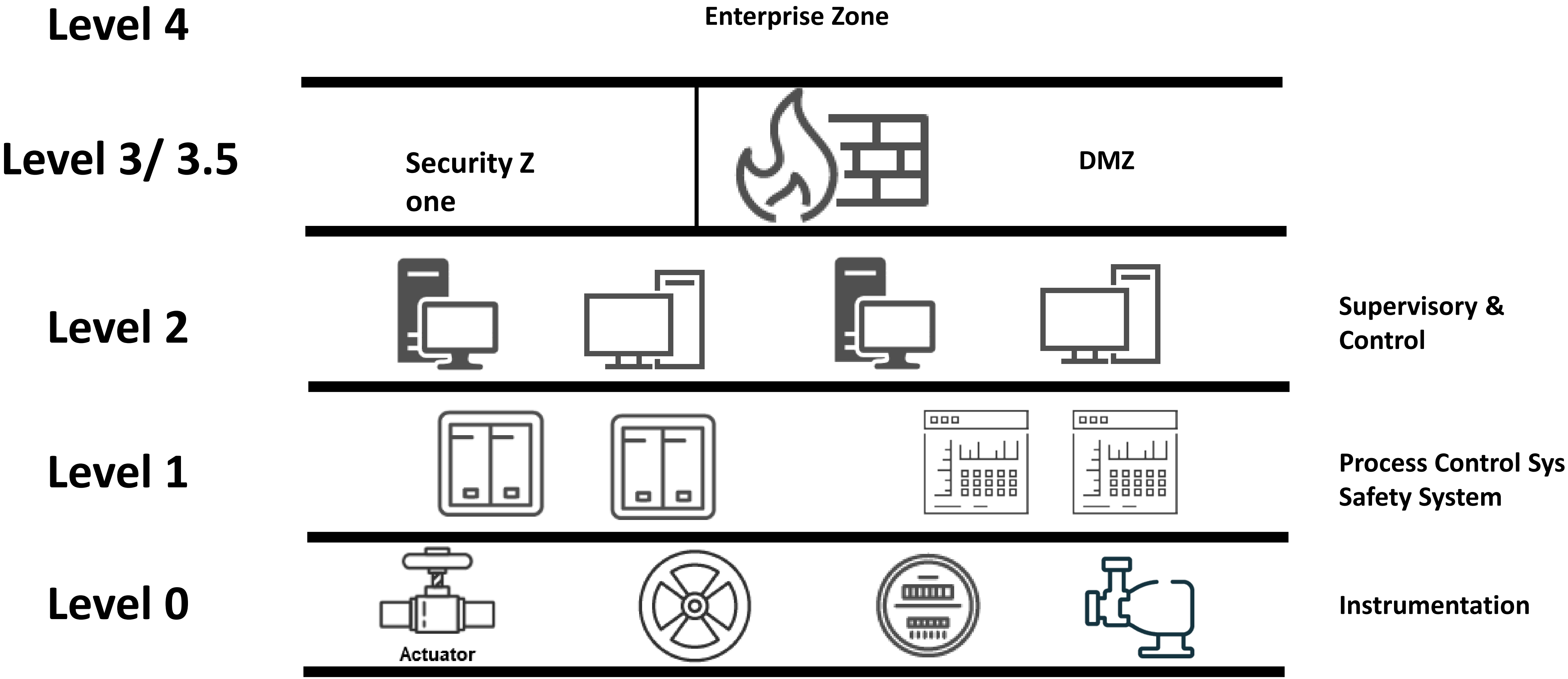
An Overview


SAUDI ARAMCO - LARGEST INTEGRATED OIL AND GAS COMPANY
9,900,000
mmbpd of crude oil production
4 Local Oil Refineries
6.4mmbpd local & global refining capacity
Offshore Operations
7.0mmbpd pipeline capacity
7.1mmbpd Avg total daily cude exports
Oil Prod
Petro Chem
Pipeline & Distribution
Refining
Gas Prod
Power
Oil facilities
Gas facilities
Petrochem cial
4.8 gigawatts
17,000 Service stations supplied

https://www.aramco.com/-/media/publications/corporate-reports/saudi-aramco-ara-2019-english.pdf

- □ Large asset owner operations can be very complex
- □ Operations require an extensive supply chain
- □ Industrial automation and control systems used in production, processing, and distribution of products
- □ Global and local regulations requiring compliance
- □ Risk related to IT/OT systems

IACS Architecture



Level 4

Enterprise Zone

Level 3/ 3.5

Security Z
one

DMZ

Level 2

Supervisory &
Control

Level 1

Process Control Sys
Safety System

Level 0

Actuator

Instrumentation

The Complexity of Securing IACS

- Legacy IACS systems
- System Diversity
- Adoption of IT systems vs. vendor proprietary systems for industrial process automation
- Operations focused on functionality and stability, rather than security
- Require 99.999% system uptime
- Systems modifications by asset owners, to address vulnerabilities, may nullify ICS vendor warranty
- Broad range of stakeholders required to confront ICS cybersecurity
- Consequences of successful cyber attack may result in loss of life or health, environmental impact, and significant financial loss

ICS Cybersecurity Compliance

What is Cybersecurity Compliance

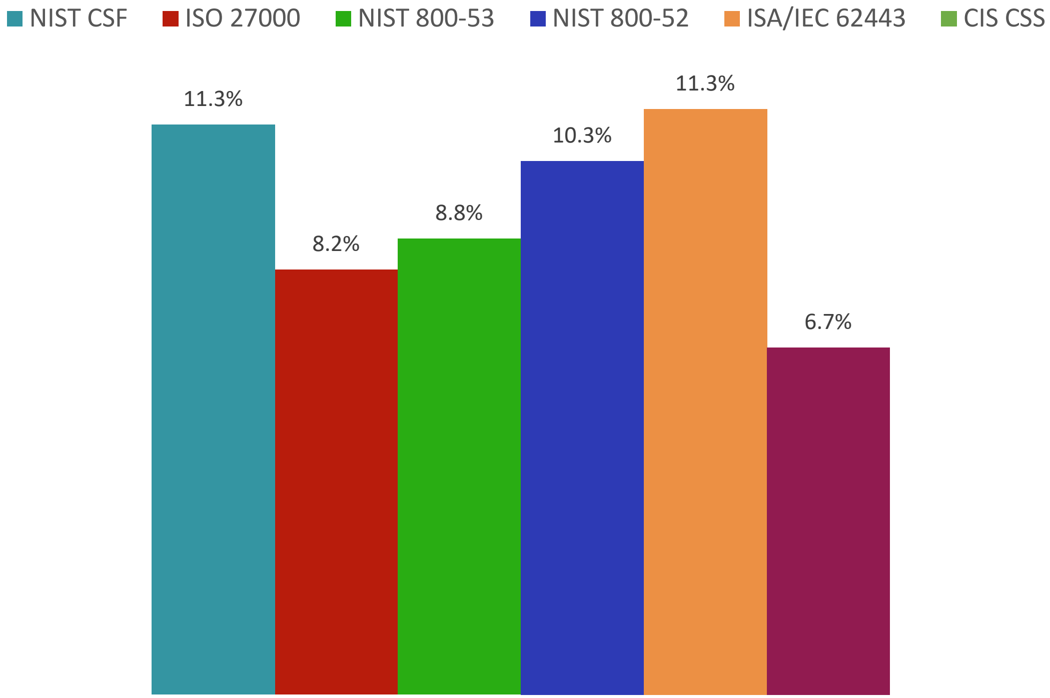
- Conformance to cybersecurity rules
- Rules otherwise known as controls or requirements originate from global standards and frameworks
- Cybersecurity controls are adopted by organizations based on risk management, regulatory mandates, operational licenses, customer requirements
- Controls usually represent minimum cybersecurity requirements
- Compliance can be measured against people, process, and technology controls

Global Standards found in IACS Environments

Top 10 Regulations, Standards, Best Practices Used

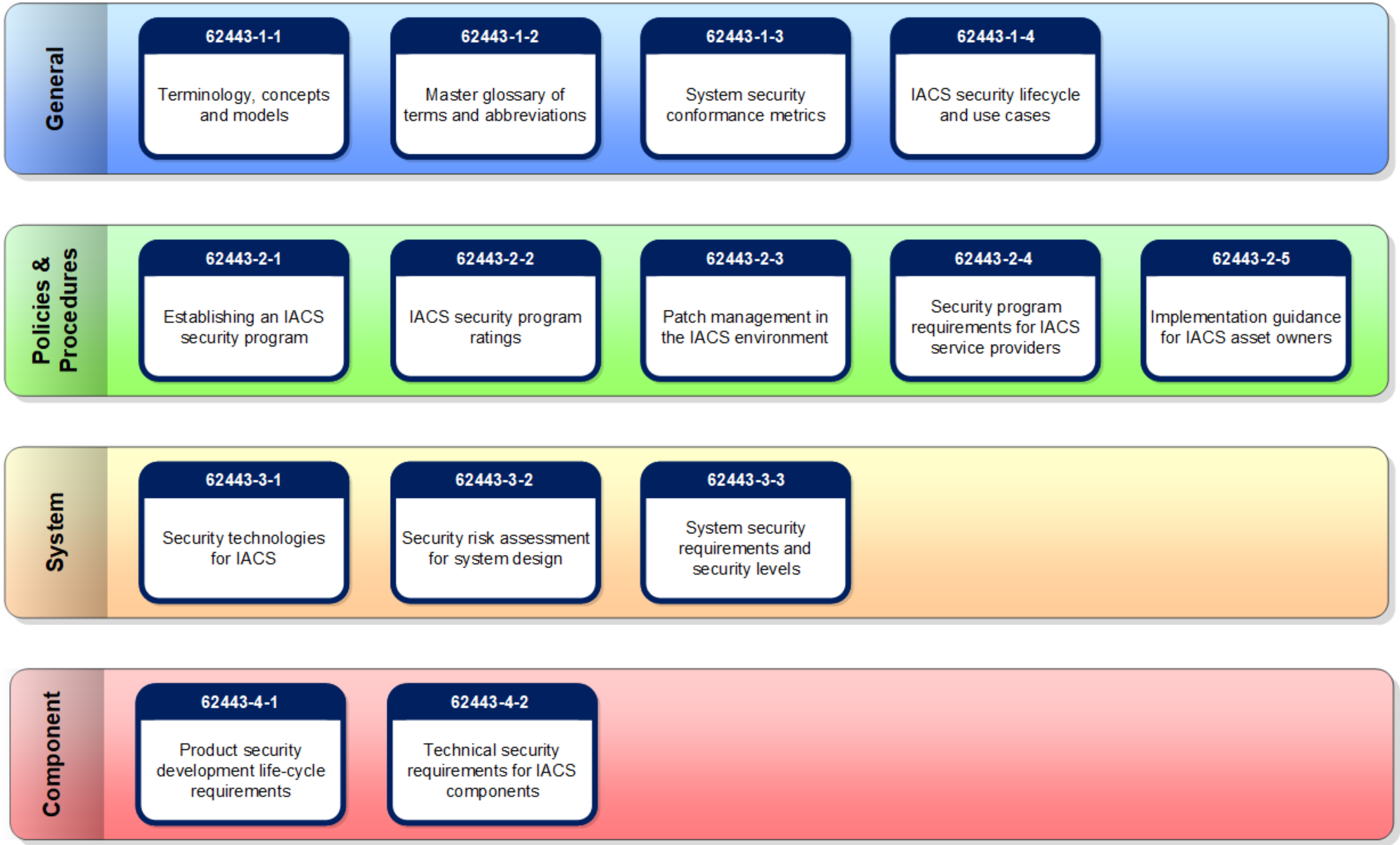
Rank	Regulation	% Response
1	NIST CSF (Cyber Security Framework)	38.1%
2	ISO 27000 series	32.0%
3	NIST 800-53	31.4%
4	NIST 800-82	30.9%
5	ISA/IEC 62443	30.4%
6	CIS Critical Security Controls	29.9%
7	NERC CIP	23.7%
8	GDPR	15.5%
9	C2M2 (Cybersecurity Capability Maturity Model)	10.3%
10	NIS Directive (EU)	8.3%

Security Standards & Regulations Mapped to OT/Control Systems



[https://www.forescout.com/company/resources/2019-sans-state-of-ot-ics-cybersecurity-survey/

ISA/IEC 62443 IACS Standard



General

62443-1-1 Terminology, concepts and models

62443-1-2 Master glossary of terms and abbreviations

62443-1-3 System security conformance metrics

62443-1-4 IACS security lifecycle and use cases

Policies & Procedures

62443-2-1 Establishing an IACS security program

62443-2-2 IACS security program ratings

62443-2-3 Patch management in the IACS environment

62443-2-4 Security program requirements for IACS service providers

62443-2-5 Implementation guidance for IACS asset owners

System

62443-3-1 Security technologies for IACS

62443-3-2 Security risk assessment for system design

62443-3-3 System security requirements and security levels

Component

62443-4-1 Product security development life-cycle requirements

62443-4-2 Technical security requirements for IACS components

- ❑ IACS Cybersecurity requirements
- ❑ Requirements for people, process, and technology
- ❑ Expanded from just the industrial process sector and applied to building automation, medical devices, and transportation sectors
- ❑ Considered the de facto standard for IACS
- ❑ Very wide global adoption
- ❑ Introduces concepts like security levels, and zone and conduits

ISASecure® Certification Scheme

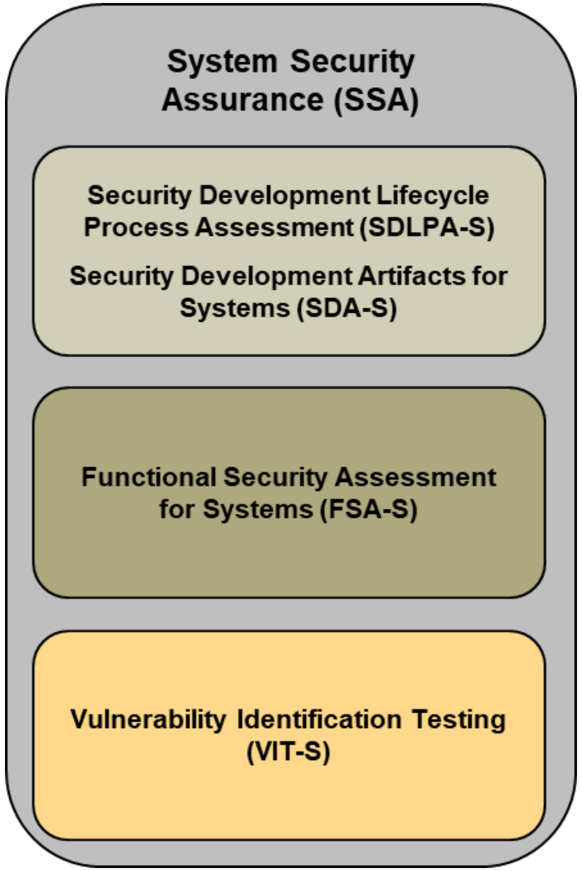
❑ Third-party conformance assessment scheme

❑ Based on the ISA/IEC 62443 series of standards

❑ ISASecure® develops and maintains the certification scheme

❑ ISASecure® certificate demonstrate compliance to applicable ISA/IEC 62443 requirements

❑ Certification establishes trust between IACS stakeholders



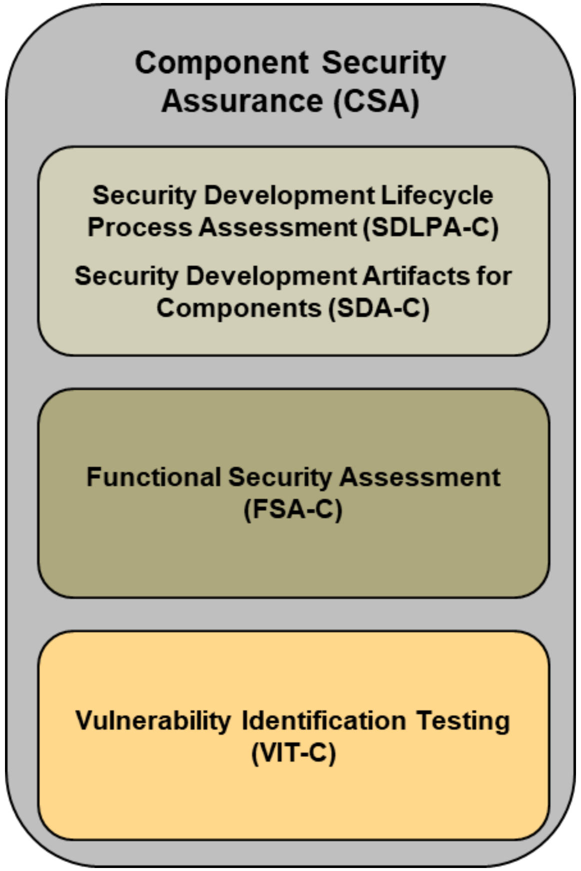
System Security Assurance (SSA)

Security Development Lifecycle Process Assessment (SDLPA-S)

Security Development Artifacts for Systems (SDA-S)

Functional Security Assessment for Systems (FSA-S)

Vulnerability Identification Testing (VIT-S)



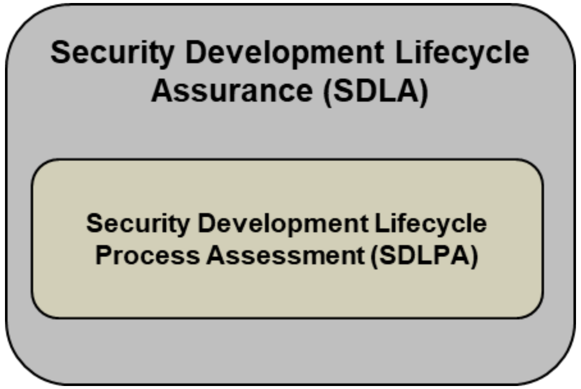
Component Security Assurance (CSA)

Security Development Lifecycle Process Assessment (SDLPA-C)

Security Development Artifacts for Components (SDA-C)

Functional Security Assessment (FSA-C)

Vulnerability Identification Testing (VIT-C)



Security Development Lifecycle Assurance (SDLA)

Security Development Lifecycle Process Assessment (SDLPA)

Compliance Control vs. Security Controls

- ❑ Requirements are usually the minimum
- ❑ Controls are based on standards and frameworks
- ❑ Regulators care about your compliance
- ❑ One-size fits all organizations
- ❑ Easy to measure and test controls
- ❑ Controls change gradually based on predefined review cycles

- ❑ Requirements are based on risk
- ❑ Controls are based on threat
- ❑ Hackers care about your security
- ❑ Unique to an organization
- ❑ More rigorous to measure and test controls
- ❑ Controls change rapidly due to threat

Compliance Myths

We are compliant, Hurray! We are finally secure … not so fast

Once compliant, always compliant

Compliance is a business inhibitor

Compliance absolves me from accountability

My automation vendor says don’t do it, now I am compliant

Compliance Assessment

Compliance Assessment Approaches

Approach	Description	Pros	Cons
Sample Set Controls Validation by an Assurance Entity	Conduct Compliance assessment by and for a subset of systems and processes	▪ Medium level of assurance ▪ Frequent assessments possible ▪ Most affordable ▪ Assurance entity personnel required is limited	▪ Pushback from entities ▪ Low level of assurance
Full Compliance Self-Validation, Sample Set Controls Validation by an Assurance Entity	Assessed entity conducts full assessments, assurance entity samples subset of systems with a full assessment	▪ Assurance entity personnel required is limited	▪ Low level of assurance ▪ Likely biased results ▪ Significant knowledge transfer required ▪ Expensive
Full Compliance Validation by an Assurance Entity	Conduct Compliance assessment for all inscope systems and processes	▪ High level of assurance ▪ High independence	▪ Resource intensive ▪ Pushback from entities ▪ Expensive
Full Compliance Self-Validation, Full Compliance Validation by an Assurance Entity	Assessed entity conducts full assessments, assurance entity conducts full review of all assessed entity assessment reports	▪ Highest level of assurance ▪ Assurance entity personnel required is limited ▪ High independence	▪ Significant knowledge transfer required ▪ Most expensive

Compliance Assessment Challenges in IACS

❑ Subjectivity

❑ Remote facilities

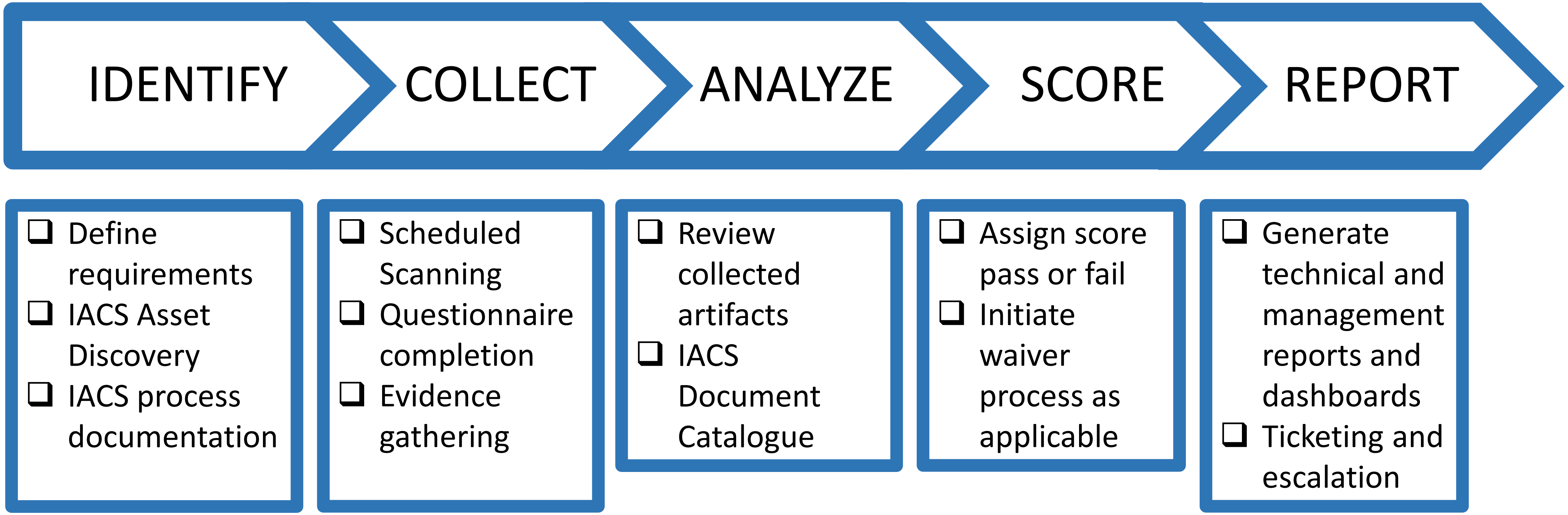
❑ High-level vs. Specific

❑ A point in-time assurance

❑ Determining inscope assets

❑ IACS Cybersecurity knowledge gap

Compliance Assessment Process Phases



IDENTIFY

- □ Define requirements
- □ IACS Asset Discovery
- □ IACS process documentation

COLLECT

- □ Scheduled Scanning
- □ Questionnaire completion
- □ Evidence gathering

ANALYZE

- □ Review collected artifacts
- □ IACS Document Catalogue

SCORE

- □ Assign score pass or fail
- □ Initiate waiver process as applicable

REPORT

- □ Generate technical and management reports and dashboards
- □ Ticketing and escalation

Compliance Automation

Compliance Automation

DEFINITION

- ❑ Consolidates asset meta data, controls, findings, workflows, scoring, reporting, and dashboards in one location
- ❑ Visualize and action all compliance assessment information in one location

BENEFITS

- ❑ Sampling not required
- ❑ Assessment frequency can increase providing greater assurance
- ❑ Less manpower required
- ❑ Significant reduction in assessment time
- ❑ Reduces potential for human error
- ❑ Keep up with new regulations
- ❑ Quick ability to test new controls
- ❑ More cost-effective, cheaper

Automation Scope

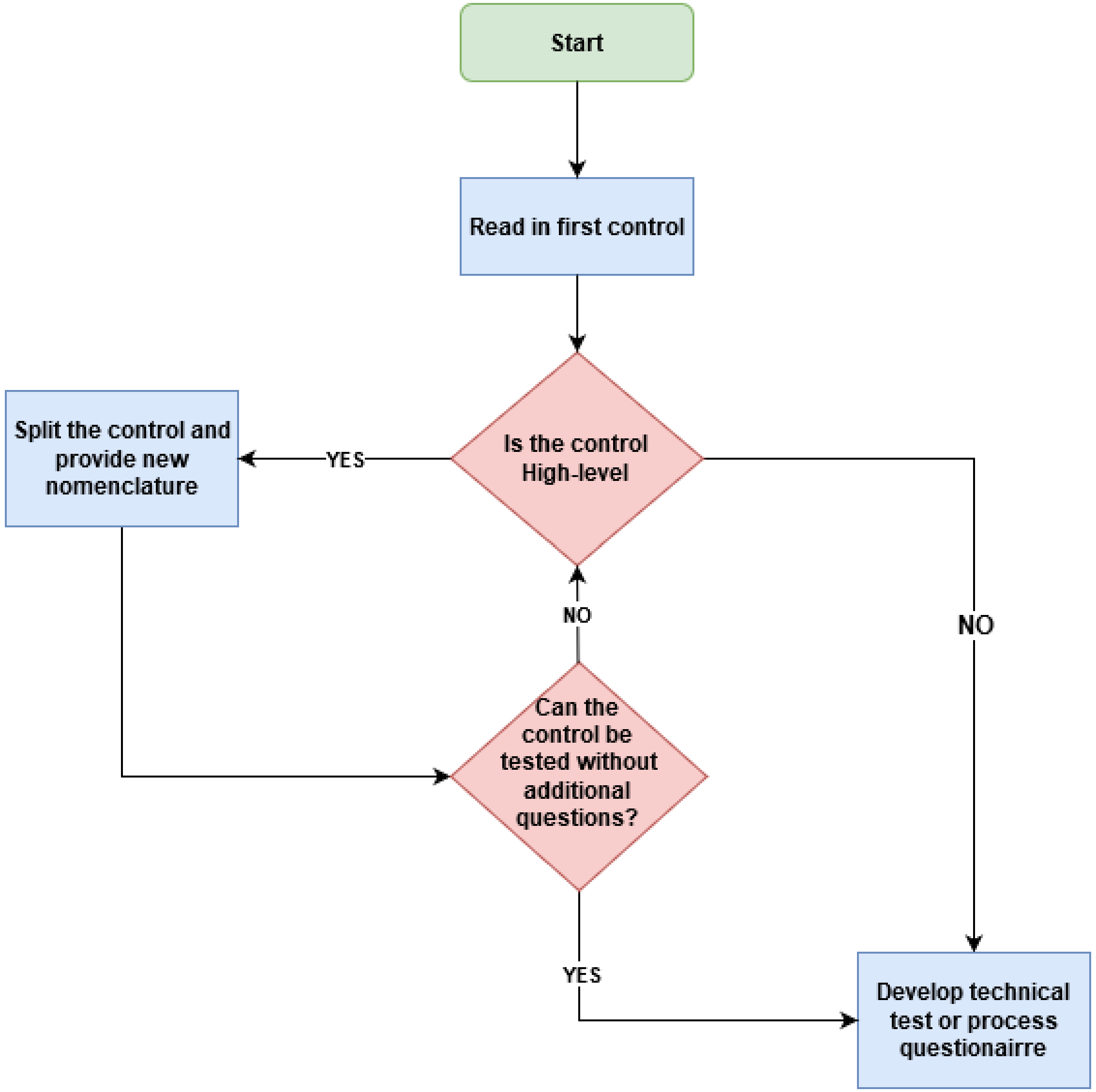
- ❑Automation occurs in some of the compliance assessment process phases
- ❑Full automation can only be truly obtained using predictive approaches

Compliance Process: Automated Phases

- ❑Identify
  - ❑Assets can be discovered automatically
  - ❑Process documentation and questionnaire completed centrally
- ❑Collect
  - ❑Scheduled systems scans for automated evidence collection
- ❑Analyze
  - ❑Automated comparison of findings
- ❑Scoring
  - ❑Automated scoring computation
- ❑Reporting
  - ❑Automated report and dashboard generation
- ❑Ticketing and Escalation
  - ❑Integration with ticketing systems for escalation

Subcontrol Development

- ❑ Compliance automation cannot occur if controls are high-level
- ❑ Simple subcontrol development process flow
- ❑ Objective is to subdivide high-level controls into binary tests
- ❑ New nomenclature is introduced and mapped to the original standard control nomenclature
- ❑ Reports will exclude newly introduced subcontrol or nomenclature
- ❑ New subcontrol and nomenclature for internal assessment process only



Start
Read in first control
Is the control High-level
YES
Split the control and provide new nomenclature
NO
NO
Can the control be tested without additional questions?
YES
Develop technical test or process questionairre

Controls & Sub-Controls Mapping

- ❑The process of accurately matching two requirements in separate standards to ensure the testing of one satisfies the other
- ❑Controls are usually done at the unit or binary level
- ❑Controls that are candidates for mapping should not be subjective
- ❑When subjective controls should be interpreted into subcontrols
- ❑ The Center for Internet Security provides a methodology and actual control mapping of their control framework to a few cybersecurity standards

Compliance Assessment Tools

Tool Advantages: Technical Assessments

	Compliance Process – NO TOOL				Compliance Process – WITH TOOL			
	IDENTIFY	COLLECT	ANALYZE	REPORT	IDENTIFY	COLLECT	ANALYZE	REPORT
Policy and Standards Management	◐				◕			
Audit and Report		◔				●		
Risk Management			◐				●	
Remediate and Track				○				●

● strong ○ weak

Scope of Automation using a Tool

- Unified control repository
- Technical Information Collection
  - Agent Based collection
  - Agentless based collection
  - Non-interactive collection
- Analysis of Expected vs. Actual
  - Verifying expected test value against received test value
  - Addressing inconclusive tests
- Consolidating and scoring
  - Grouping of tests
  - Scoring
- Reporting
  - Technical reports
  - Management KPIs
  - Ticketing and escalation