Reconciling Cybersecurity Standards

MLM-013-D

Industry	– All
Principal Role	– All
Professional Role	– All
Enterprise Phase	– All

Turn on your audio and click start to begin video

START

This MLM describes the process of reconciling cybersecurity standards for use in a corporation and its facilities and projects.

Click the NEXT button when you are ready to advance to the next slide.

There are Many Cybersecurity Standards

- Some are intended for use in all Enterprises (e.g., IEC/ISA 62443 and ISO 27001)
- Some are industry-specific (e.g., IEC 63452 for railways)
- Some are specific to one nation (e.g., NIST 800, NAMUR, CISA)
- Others are intended for use in many countries (e.g., ISO, CRA, CIS)
- Some apply to only part of the Enterprise Architecture (e.g., ISA/IEC 62443 for Automation and Control Systems, or ISA 112 for SCADA systems)
- Virtually all of these cybersecurity standards have requirements that conflict with other standards
- It is therefore necessary for each enterprise to determine which standards it should apply.
- This necessitates a corporate program to select and implement the cybersecurity policies, practices, and work processes for use in its facilities and projects.

Click Here for a list of cybersecurity standards by country and category

2

There are many cybersecurity standards.

Some are intended for use in all Enterprises (e.g., IEC/ISA 62443 and ISO 27001)

Some are industry-specific (e.g., IEC 63452 for railways)

Some are specific to one nation (e.g., NIST 800, NAMUR, CISA)

Others are intended for use in many countries (e.g., ISO, CRA, CIS)

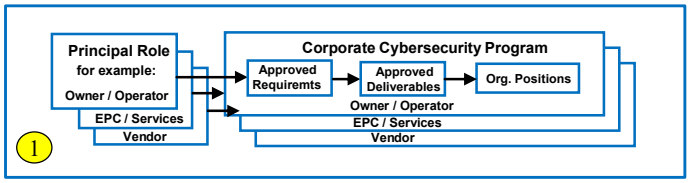
Some apply to only part of the Enterprise Architecture (e.g., ISA/IEC 62443 for Automation and Control Systems, or ISA 112 for SCADA systems)

Virtually all of these cybersecurity standards have requirements that conflict with other standards

It is therefore necessary for each enterprise to determine which standards it should apply.

This necessitates a corporate program to select and implement the cybersecurity policies, practices, and work processes for use in its facilities and projects.

Simplified Cybersecurity Principal Roles and Programs



- ISA 62443 defines "Principal Roles" including Owner/Operator, Service Providers, Device or System Suppliers, and Vendors.
- Each Principal Role prepares its own IACS Cybersecurity Program, including a set of Approved Requirements and Deliverables that are assigned to Org. Chart Positions in that Corporation.

3

ISA 62443 defines "Principal Roles" including:

- Enterprise Owner/Operator,
- Service Providers (like Engineering Contractors, System Integrators, or Maintenance Providers, and
- Device and System Suppliers and Vendors
- Ancillary Principal Roles may also be involved, including insurers, regulators, and educators, but these will not be discussed here.

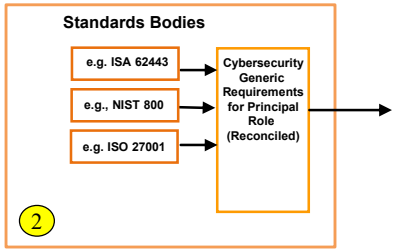
Each Principal Role should establish its own Corporate IACS Cybersecurity Program that includes:

- A set of Approved Requirements (that have been established based on Risk and Costs).
- A set of Approved Deliverables that satisfy all Approved Requirements.

These Approved Deliverables are then assigned to Organization Chart Positions within the Corporation responsible for executing the Work Processes associated with each Deliverable.

Standards Bodies Define Requirements Associated with Principal Roles

- Standards bodies define “Requirements” associated with Principal Roles. These are selected by the Principal Role (e.g. Owner/Operator) and then ”reconciled” to eliminate conflicts and produce a single set of Requirements to include in the Master Plan.



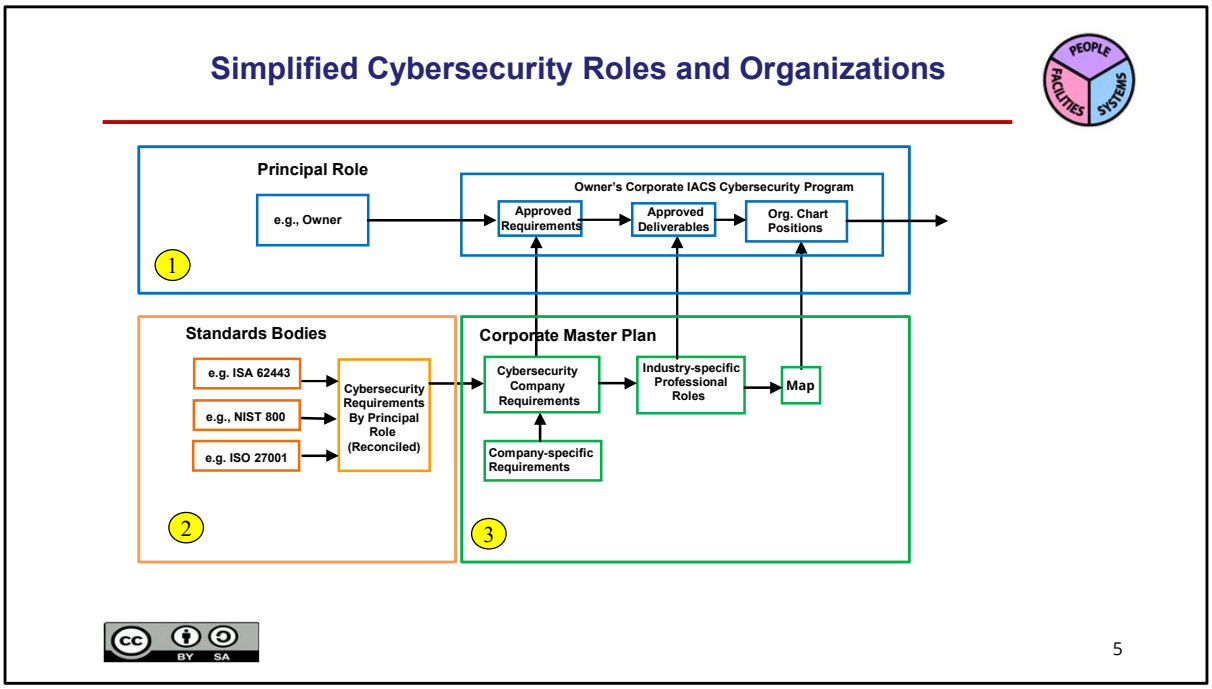
- Generic Requirements are assigned to
- “Generic Requirements and Professional Roles” apply to all enterprises
- A secondary set of Requirements and Roles are specific to individual industries.

4

Standards bodies such as ISA 62443, NIST 800, and ISO 27001 define cybersecurity “Requirements”.

These are selected by the Principal Role (e.g., Owner/Operator) and then ”reconciled” to eliminate conflicts and produce a single set of Requirements to include in the Master Plan.

ISA 62443 is intended to IACS across all enterprises. It is therefore necessary to identify “Generic Requirements and Professional Roles” that apply to all enterprises, plus a secondary set of Requirements and Roles that are specific to individual industries.



ISA 62443 defines "Principal Roles" including:

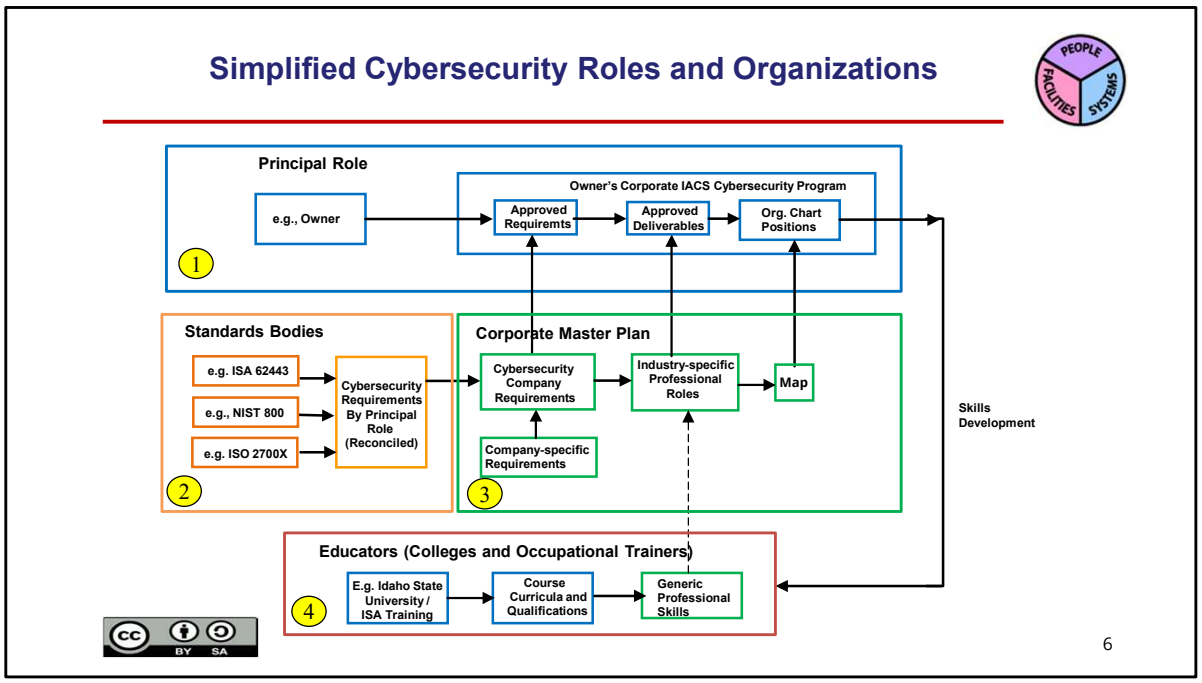
- the facility Owner/Operator,
- Service Providers (like Engineering Contractors, System Integrators, or Maintenance Providers, and
- Device and System Suppliers and Vendors

Ancillary Roles may also be involved including insurers, regulators, but these will not be discussed here.

Each of these Principal Roles should establish their own Corporate IACS Cybersecurity Program that includes:

- A set of Approved Requirements (that have been established based on Risk and Costs).
- A set of Approved Deliverables that satisfy all Approved Requirements.

These Approved Deliverables are then assigned to Org Chart Positions in the Corporation that are responsible for accomplishing the Work Processes associated with each Deliverable.



- Educational Institutions have the role of supplying industry with the necessary skilled personnel to address the roles described above.
- Both degree-granting Educational Bodies like Idaho State University, and vocational training organizations like ISA are preparing Course Curricula and Qualification Programs.
- These courses are intended to provide the Skills that Corporations will need to address the Generic Professional Roles and Industry-specific Roles identified by cybersecurity standards organizations.
- It should be noted, however, that educational institutions must imbue generic skills that are not specific to a given Principal Role and that apply across industries.
- A "skills development" program is underway to assess the skills required by corporations as part of their IACS cybersecurity programs. For example, INL and Idaho State University are collaborating on development of the CyberChamp program to assist with providing the necessary skills requirement feedback to educational bodies. ISA, by contrast obtains this feedback through dialog with companies sending employees to vocational courses provided by ISA Education

group.

Key Messages

The following are key messages in this MLM:

- Cybersecurity Requirements are selected from ISA 62443, ISO 27001, and other standards and included in the Corporate IACS Cybersecurity Program.
- Requirements in the ACS cybersecurity Program result in Engineering Deliverables that are produced by Org Chart Positions according to work processes developed by the Principal Role (e.g., Corporation)
- Generic and Industry-specific roles are assigned to Org Chart Positions
- Skills and the associated courses required to accomplish Generic and Industry-specific roles are established by Education bodies with feedback from corporations, including Owners, Service Providers, and Vendors.

The following are key messages in this MLM:

Cybersecurity Requirements defined by ISA 62443 and other standards are selected for inclusion in the Corporate IACS Cybersecurity Program.

Requirements in the IACS cybersecurity Program result in Deliverables that are produced by Org Chart Positions according to work processes developed by that Corporation

Generic and Industry-specific roles are assigned to Org Chart Positions

Skills and the associated courses required to accomplish Generic and Industry-specific roles are established by Education bodies with feedback from corporations including Owners, Service Providers and Vendors.

Further Information

These MLMs provide more information on important concepts:

- MLM-001-A Principal Roles in IACS Cybersecurity
- MLM-001-B Professional Roles in IACS Cybersecurity
- MLM-004-A Industry Classification for IACS Cybersecurity
- MLM-013-A What is an IACS Cybersecurity Program?

Please click here to provide us feedback on this learning module.

The following MLMs provide more information on important concepts:

MLM-001-A Principal Roles in IACS Cybersecurity
MLM-001-B Professional Roles in IACS Cybersecurity
MLM-004-A Industry Classification for IACS Cybersecurity
MLM-013-A What is an IACS Cybersecurity Program?

Please click here to provide us feedback on this learning module.

Author

Gary has more than 40 years of experience with enterprise integration and optimization projects, including PERA master planning and project management.

As one of the initial authors of the PERA Handbook of Master Planning, he has used PERA Enterprise Architecture and Master Planning methodologies throughout his career including control and information systems for oil production, pipelines, refining and marine loading, petrochemicals, coal, gas, and oil-fired power plants, polyethylene, ammonia, explosives, paint, pulp and paper, food and beverage, and pharmaceuticals. LNG facilities included world-scale arctic, European, and US Gulf coast complexes.

infrastructure facilities included Fire, Police, and Emergency Response systems for major US cities, as well as emissions reporting and trading systems for more than 100 US Power Plants,

Gary has more than 40 years of experience with enterprise integration and optimization projects, including PERA master planning and project management.

As one of the initial authors of the PERA Handbook of Master Planning, he has used PERA Enterprise Architecture and Master Planning methodologies throughout his career including control and information systems for oil production, pipelines, refining and marine loading, petrochemicals, coal, gas, and oil-fired power plants, polyethylene, ammonia, explosives, paint, pulp and paper, food and beverage, and pharmaceuticals. LNG facilities included world-scale Arctic, European, and US Gulf coast complexes.

infrastructure facilities included Fire, Police, and Emergency Response systems for major US cities, as well as emissions reporting and trading systems for more than 100 US Power Plants,