

# The RIPE Crosswalk

Comparing the RIPE cyber security program  
to ICS security standards and frameworks

Perry Pederson

November 2014



**Content**

Summary ..... 3

Introduction..... 3

ISA-99/IEC-62443 ..... 5

NERC CIP (Critical Infrastructure Protection) ..... 8

NRC Regulatory Guide 5.71 ..... 11

NEI 08-09 Cyber Security Plan for Nuclear Power Reactors..... 14

ISO 27000 ..... 17

WIB Process Control Domain Vendor Requirements..... 20

DOE Cybersecurity Capability Maturity Model (C2M2) ..... 23

NIST Cyber Security Framework (CSF)..... 26

## Summary

For some critical infrastructure sectors (e.g., chemical, nuclear) compliance to standards is driven by regulations while other sectors are driven by industry best practices or business necessity. In any case, high-level standards and requirements usually provide the aiming point for cyber security efforts.

This paper provides a high-level comparison of The Langner Group's Robust ICS Planning and Evaluation (RIPE) Program to major cyber security frameworks or standards. It is pointed out how its key characteristics map to existing frameworks, and where it may even exceed such frameworks.

A major difference that emerges is the level of detail that RIPE provides, along with annual improvements and information sharing that are driven by a private corporation (The Langner Group). It is suggested to asset owners to employ RIPE as the preferred method of implementing their respective high-level cyber security framework, standard, or regulatory requirements.

## Introduction

With so many cyber security standards and frameworks by international standard bodies, government agencies, and industry associations around, one might question why we need yet another "standard" – the RIPE cyber security program – developed by a private corporation. The simple answer is that no existing standard or framework passed the test of practicality. Asset owners are anything but eager to adopt and implement any of the existing approaches because they have realized how much labor and budget is required to make it happen. And since guesswork is involved too, because detailed procedures are lacking, it cannot even be taken for granted that a best-meaning implementation would be "correct" in all its aspects, not even speaking about arriving at a reasonably secure configuration at the end of the day.

The simple reason for such trouble is that none of the existing standards was actually meant and developed as a hands-on, detailed procedural document, but rather as high-level guidance documents. It wouldn't even be reasonable to expect concrete hands-on help from government agencies or standard bodies, if only for the fact that it implies the identification of configuration and product specific issues that change over time. A nuclear regulator, for example, does not have the resources or the procedures to keep track with such developments, and to address them in something that basically looks like a commercial product that is continuously improved based on customer feedback. A private corporation does. This is the basic value proposition of the RIPE cyber security program, and the business model of its developer (The Langner Group).

RIPE does not pretend to be another "standard" that would rival, for example, ISA-99 or the NIST Cyber Security Framework. Nor is there an effort to suggest that RIPE can replace any of these standards. Instead, it bridges the gap between the high-level guidance that such documents provide and the actual procedures and solutions that they call for on the plant floor. RIPE can fill the "how-to" gap in all of the existing approaches. In other words, RIPE provides the detailed step-by-step implementation of **a sustainable, measurable, and cost-efficient ICS cyber security governance process**.

The purpose of this document is to document how the various parts of RIPE map to each of the major cyber security standards and frameworks covered to give the reader a better idea how "his" or "her" preferred or mandated standard is reflected in RIPE. There is no intention to imply an exact match

between specific requirements. In all cases, the comparison is based on the currently available version of each framework or standard.

As the reader will see, RIPE does include aspects that are not or only partly addressed by certain standards. These are also pointed out throughout the document. In general, there is a simple reason why RIPE goes beyond existing guidance in some cases:

It is usually out of scope for a government agency or standards body to focus on the economical aspects of cyber security programs, especially on their **cost-efficiency, sustainability, and measurability**.

Asset owners, on the other hand, cannot exclude these characteristics for obvious reasons. Wasting company resources on cyber security is easy, spending cyber security dollars for maximum return and hard numbers to prove it is difficult. For example, any ICS security strategy that ignores the role of the supply chain cannot be sustainable (insecure-by-design products will continue to be commissioned and call for after-the-fact “band-aid” style security controls). For this reason, RIPE may supplement particular guidelines with information on how to address system procurement, and with a product catalog (database) that lists cyber security characteristics of existing products that is accessible by RIPE users. Another example is ICS security metrics that are absent in the majority of existing standards. Based on the old wisdom that one cannot improve what one cannot measure, metrics are a core element of RIPE.

The following table provides a quick overview on how key features and characteristics of RIPE are shared with various standards.

		RIPE	ISA 99	NERC CIP	RG 5.71	NEI 08-09	ISO 27000	WIB	DOE C2M2	NIST CSF
<b>RIPE Functions &amp; Attributes</b>	Governance	Green	Yellow	Yellow	Green	Green	Green	Red	Red	Yellow
	Metrics	Green	Yellow	Red	Red	Red	Green	Yellow	Red	Red
	Structural & Behavioral System Model	Green	Red	Red	Red	Red	Yellow	Red	Red	Red
	Cyber Security Capability Development	Green	Red	Red	Red	Red	Red	Red	Green	Red
	Ready-to-use Templates	Green	Red	Red	Yellow	Yellow	Red	Red	Red	Red
	Information Sharing on Problems & Progress	Green	Red	Red	Red	Red	Red	Red	Green	Yellow
	Cross-industry Approach	Green	Green	Red	Red	Red	Green	Yellow	Yellow	Green
<b>RIPE Domains</b>	System Population Characteristics	Green	Yellow	Yellow	Green	Green	Red	Green	Green	Green
	Network Architecture	Green	Red	Red	Green	Red	Red	Yellow	Yellow	Red
	Component Interaction	Green	Yellow	Red	Yellow	Yellow	Red	Green	Red	Yellow
	Workforce Roles and Responsibilities	Green	Red	Red	Green	Green	Red	Yellow	Green	Green
	Workforce Skills & Competence Development	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Green
	Procedural Guidance (Policies & SOPs)	Green	Green	Green	Green	Green	Red	Yellow	Yellow	Green
	Deliberate Design Change	Green	Green	Green	Green	Green	Yellow	Green	Green	Yellow
System Acquisition	Green	Green	Red	Yellow	Red	Red	Green	Green	Red	

Significant differences ■  
 Some elements in common ■  
 Significant similarities ■

## ISA-99/IEC-62443

Developed by	International Society of Automation’s (ISA) Committee for Industrial Automation and Control Systems Security, also adopted by the International Electrotechnical Commission (IEC).
Overview	ISA-99 is the attempt to map the ISO 27000 standards to industrial control system environments.
Applies to	Manufacturing and process industries
Hyperlink	<a href="https://www.isa.org/isa99/">https://www.isa.org/isa99/</a>

	RIPE	ISA-99/IEC-62443
<b>RIPE Functions</b>		
Governance	A continuous process that determines the accuracy and completeness of system documentation, and measures and enforces compliance to procedural directives periodically.	A cyber security management system (CSMS) includes all the measures necessary to create, maintain, monitor determine effectiveness, and improve the CSMS. Provides other sources to address governance: Corporate Governance Task Force “Information Security Governance – A call to action.”
Metrics	<p>Metrics used to measure completeness, and one of the following for each of the eight RIPE domains:</p> <ul style="list-style-type: none"> <li>• accuracy,</li> <li>• compliance, or</li> <li>• conformity.</li> </ul> <p>RIPE also provides metrics for measuring RIPE documentation, policies, as well as an overall index of cyber security capability.</p>	Provides general guidelines for developing programmatic metrics. However, ISA–99.02.02 (a future publication) is intended to include the definition and application of metrics to measure program effectiveness. Currently, there is no generally accepted means to measure the effectiveness of cyber security programs, objectives, or controls. For example, was the control effective or did the hackers just decide to take a holiday?
Structural & Behavioral System Model	Developing a detailed structural and behavioral ICS model is essential to complete system understanding. Using the information from the system inventory, network architecture diagrams, and dataflow diagrams, a detailed structural and behavioral model is developed which supports advanced vulnerability analysis.	Describes a series of models that are used to apply the basic concepts of security for industrial automation and control systems. It does not provide guidance on how to build a model of an existing system with enough fidelity to allow detailed vulnerability analysis.
Cyber Security Capability Development	Not only does every element in RIPE support developing cyber security capability, but the metrics to actually measure current state as well as progress toward a desired end state.	Within the context of ISA/IEC the term 'capability' is typically applied at the component level. Capability SALs (security assurance levels) are the security levels that component or systems can provide when properly configured. However, whatever organizational or programmatic capability that may exist or be developed following ISA/IEC guidance will be severely hampered at the start because all efforts will be framed by a risk assessment.
Ready-to-use Templates	Four of the eight RIPE domains are prescriptive with templates and guidance on a Training Curriculum,	Although the use of templates are recommended to bring conformity and ease of use, none are provided.

	System Procurement, Plant Planning, as well as Policies and Standard Operating Procedures. These templates are provided and then customized in close cooperation with stakeholders.	
Information Sharing on Problems & Progress	Every aspect of RIPE, in particular vulnerability mitigation and the concept of continuous improvement, are enhanced through a process of peer-to-peer information sharing. Nonetheless, RIPE licensees may elect not to share and hence not receive any benefit therefrom.	There is an information-sharing format based on XML for communicating the testing and approval of patches for installation.
Cross-industry Approach	RIPE favors a cross-industry approach from the start, by focusing on providing a generic security capability baseline. Within the RIPE instruments rules are written in a way that allows for extension of generic to industry specific to application specific to version specific. Furthermore, benchmarking cross-industry is only possible when metrics are applied in a systematic and standard way. RIPE provides a means to make cross-industry benchmarking possible through objective standardized measurements of security posture.	Although benchmarking cross-industry is not integral to the standard, users may find cooperative partners within their industry segment or in other industries. However, effective benchmarking is only possible when a cyber security program and metrics are applied in a systematic and standard way.
<b>RIPE Domains</b>		
System Population Characteristics	Detailed equipment and instrument list (cyber system inventory), manifested as a database, stores information on hardware systems, the software running on those systems, network association, and configuration details.	Requires taking an inventory of industrial automation and control systems (IACS) systems, networks, and devices. However, ISA99 also caveats this requirement suggesting that resource or time constraints may not allow detailed examination of all of these assets.
Network Architecture	A network architecture model, manifested as a set of diagrams with accompanying detail information for reference, identifies the connectivity options for specific endpoints and groups of endpoints. It identifies which network-connected systems can talk to which other network-connected systems.	The organization shall develop simple network diagrams for each of the logically integrated systems showing the major devices, network types, and general locations of the equipment. ISA99 provides reference architectures for IACS, SCADA, as well as corporate environments with more specific segmentation guidance based on risk level.
Component Interaction	Process flow diagrams with accompanying detail information, identifies the interfaces of digital components. For interfaces that have dedicated communication counterparts, such association is identified. Interfaces extend to non-IP networks, fieldbus, RS-232, and proprietary.	The [process flow] diagram should attempt to capture the basic logical network architecture, such as connectivity approaches, combined with some of the physical network architecture basics like location of devices. Simple network diagrams are a starting point and should not form the sole basis for assessing connectivity without more detailed physical validation.
Workforce Roles and Responsibilities	Workforce records of personnel. Identities, affiliation (staff or contractor), role-based physical and logical access and execution privileges, applicable policies and	Requires written policies and procedures that allow employees, contractors, third parties, and others to clearly understand a company's perspective of cyber security and their <u>roles and responsibilities</u> in securing the

	SOPs, and competence of all individuals that legitimately interact with industrial control and safety systems or process IT equipment.	company's assets. ISA99 also requires an integrated approach for access control because of its central role in securing the IACS network.
Workforce Skills and Competence Development	Training curriculum and records of operations and maintenance personnel is a requirement that documents staff members and contractors' ability to perform their interactions with industrial control systems professionally and meet the provisions of policies and SOPs.	Records of employee training and schedules for training updates should be maintained and reviewed on a regular basis. To ensure that personnel remain competent in their roles and responsibilities, all personnel should receive adequate technical training associated with the known threats and vulnerabilities of hardware, software and social engineering.
Procedural Guidance	Standard operating procedures used by operations and maintenance personnel for cyber, manifested as written documents, structure the activities that comprise legitimate and appropriate interaction with plant floor systems.	The organization shall develop and approve cyber security procedures, based on the cyber security policies, and provide guidance in how to meet the policies. These written policies and <u>procedures</u> that allow employees, contractors, third parties, and others to clearly understand a company's perspective of cyber security and their roles and responsibilities in securing the company's assets.
Deliberate Design and Configuration Change	Plant planning and change management procedures for cyber on the topology and architecture of process networks, configuration of essential infrastructure services, authorized remote access options and products, or proper configuration and usage of virtualization technology.	A change management system for the IACS environment shall be developed and implemented. Requires confirming the security, availability, and usability of the control system configuration. This includes the logic used in developing the configuration or programming for the life of the industrial automation and control system.
System Acquisition	System procurement guidelines specifying physical and functional system attributes and properties that industrial control and safety systems, industrial network gear, and process IT systems must have in order to meet an organization's quality criteria.	The security functions and capabilities of each new component of the IACS shall be defined up front, developed or achieved via procurement, and tested together with other components so that the entire system meets the desired security profile. Applies to the maintenance of existing systems as well as procurement of new systems.

## NERC CIP (Critical Infrastructure Protection)

Developed by	North American Electric Reliability Corporation (NERC)
Overview	The NERC CIP Standards address the security of cyber assets essential to the reliable operation of the electric grid. To date, these standards (and those promulgated by the Nuclear Regulatory Commission) are the only mandatory cybersecurity standards in place across the critical infrastructures of the United States.
Applies to	US electrical power industry
Hyperlink	Complete set of NERC reliability standards (which includes all of the CIP standards): <a href="http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSC%20CompleteSet.pdf">http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSC%20CompleteSet.pdf</a>

	RIPE	NERC CIP
<b>RIPE Functions</b>		
Governance	A continuous process that determines the accuracy and completeness of system documentation, and measures and enforces compliance to procedural directives periodically.	Tangential reference is made to governance rather than as a specific requirement with an analog in a Cyber Security Policy and Compliance Monitoring Process. The CIP Senior Manager is expected to play a role in ensuring overall program governance.
Metrics	<p>Metrics used to measure completeness, and one of the following for each of the eight RIPE domains:</p> <ul style="list-style-type: none"> <li>• accuracy,</li> <li>• compliance, or</li> <li>• conformity.</li> </ul> <p>RIPE also provides metrics for measuring RIPE documentation, policies, as well as an overall index of cyber security capability.</p>	No guidance on security performance metrics is provided. However, measures (e.g., documentation) are the evidence that could be presented to demonstrate compliance and are not intended to contain the quantitative metrics for determining satisfactory performance nor to limit how an entity may demonstrate compliance if valid alternatives to demonstrating compliance are available in a specific case.
Structural & Behavioral System Model	Developing a detailed structural and behavioral ICS model is essential to complete system understanding. Using the information from the system inventory, network architecture diagrams, and dataflow diagrams, a detailed structural and behavioral model is developed which supports advanced vulnerability analysis.	No structured nor behavioral ICS system model is required. However, models that represent the baseline configuration prior to implementing a change that deviates from that baseline are required noting that the requirement is to “model” the baseline configuration and not duplicate it exactly.
Cyber Security Capability Development	Not only does every element in RIPE support developing cyber security capability, but the metrics to actually measure current state as well as progress toward a desired end state.	The CIP requirements assumes a cyber security capability exists, but only provides for qualitative assessments as opposed to quantitative measurements of that capability.
Ready-to-use Templates	Four of the eight RIPE domains are prescriptive with templates and guidance on a Training Curriculum, System Procurement, Plant Planning, as well as Policies and Standard Operating Procedures. These templates are provided and then customized in close cooperation with	Does not contain end user templates, but there are many options available from third-parties and consultants.

	stakeholders.	
Information Sharing on Problems & Progress	Every aspect of RIPE, in particular vulnerability mitigation and the concept of continuous improvement, are enhanced through a process of peer-to-peer information sharing. Nonetheless, RIPE licensees may elect not to share and hence not receive any benefit therefrom.	Although peer-to-peer information sharing is not integral to the NERC CIP, users must develop and apply a process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) either directly or through an intermediary.
Cross-industry Approach	RIPE favors a cross-industry approach from the start, by focusing on providing a generic security capability baseline. Within the RIPE instruments rules are written in a way that allows for extension of generic to industry specific to application specific to version specific. Furthermore, benchmarking cross-industry is only possible when metrics are applied in a systematic and standard way. RIPE provides a means to make cross-industry benchmarking possible through objective standardized measurements of security posture.	Benchmarking cross-industry is only possible when a cyber security program and metrics are applied in a systematic and standard way. NERC CIP is only applied in one industry and therefore, cross-industry comparisons are not possible.
<b>RIPE Domains</b>		
System Population Characteristics	Detailed equipment and instrument list (cyber system inventory), manifested as a database, stores information on hardware systems, the software running on those systems, network association, and configuration details.	Identify and document a risk-based assessment methodology to identify Critical Assets and a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Review this list at least annually, and update it as necessary.
Network Architecture	A network architecture model, manifested as a set of diagrams with accompanying detail information for reference, identifies the connectivity options for specific endpoints and groups of endpoints. It identifies which network-connected systems can talk to which other network-connected systems.	Although not specifically called for in the requirement, examples of compliance to the requirement may include, but are not limited to, network diagrams or architecture documents.
Component Interaction	Process flow diagrams with accompanying detail information, identifies the interfaces of digital components. For interfaces that have dedicated communication counterparts, such association is identified. Interfaces extend to non-IP networks, fieldbus, RS-232, and proprietary.	Although not specifically called for in the requirement, examples of compliance to the requirement may include, but are not limited to, network diagrams or architecture documents.
Workforce Roles and Responsibilities	Workforce records of personnel. Identities, affiliation (staff or contractor), role-based physical and logical access and execution privileges, applicable policies and SOPs, and competence of all individuals that legitimately interact with industrial control and safety systems or process IT equipment.	Four out of eleven (36%) of the NERC CIPs specifically require the definition of roles and responsibilities.

<p>Workforce Skills and Competence Development</p>	<p>Training curriculum and records of operations and maintenance personnel is a requirement that documents staff members and contractors' ability to perform their interactions with industrial control systems professionally and meet the provisions of policies and SOPs.</p>	<p>To minimize the risk against compromise that could lead to misoperation or instability from individuals accessing Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting Cyber Systems.</p>
<p>Procedural Guidance</p>	<p>Standard operating procedures used by operations and maintenance personnel for cyber, manifested as written documents, structure the activities that comprise legitimate and appropriate interaction with plant floor systems.</p>	<p>The term documented processes refers to a set of required instructions specific to the organization and to achieve a specific outcome. As such, documented processes are required in nine out of eleven (82%) of the NERC CIPs.</p>
<p>Deliberate Design and Configuration Change</p>	<p>Plant planning and change management procedures for cyber on the topology and architecture of process networks, configuration of essential infrastructure services, authorized remote access options and products, or proper configuration and usage of virtualization technology.</p>	<p>Establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software. Implement configuration management activities to identify, control and document entity or vendor related changes to hardware and software components of Critical Cyber Assets.</p>
<p>System Acquisition</p>	<p>System procurement guidelines specifying physical and functional system attributes and properties that industrial control and safety systems, industrial network gear, and process IT systems must have in order to meet an organization's quality criteria.</p>	<p>No guidelines or criteria provided in the NERC CIPs.</p>

## NRC Regulatory Guide 5.71

Developed by US Nuclear Regulatory Commission (NRC)

Overview Regulatory Guide 5.71 (RG 5.71) is the NRC’s guideline for one possible way to implement the requirements set forth in 10 CFR 73.54 which requires licensees to provide high assurance against cyber attacks.

Applies to US nuclear power plants

Hyperlink <http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf>

	RIPE	RG 5.71
<b>RIPE Functions</b>		
Governance	A continuous process that determines the accuracy and completeness of system documentation, and measures and enforces compliance to procedural directives periodically.	Develop, review (1-year cycle) and update a formal, documented security planning, assessment and authorization policy that describes the purpose, scope, roles, responsibilities, management commitments, and coordination and implementation of a cyber security program.
Metrics	<p>Metrics used to measure completeness, and one of the following for each of the eight RIPE domains:</p> <ul style="list-style-type: none"> <li>• accuracy,</li> <li>• compliance, or</li> <li>• conformity.</li> </ul> <p>RIPE also provides metrics for measuring RIPE documentation, policies, as well as an overall index of cyber security capability.</p>	<p>No programmatic level metrics, but recommends:</p> <ul style="list-style-type: none"> <li>• Measuring the cyber incident response capability within the organization</li> <li>• Measuring vulnerability impact</li> <li>• Developer security metrics for defect tracking within the code</li> </ul>
Structural & Behavioral System Model	Developing a detailed structural and behavioral ICS model is essential to complete system understanding. Using the information from the system inventory, network architecture diagrams, and dataflow diagrams, a detailed structural and behavioral model is developed which supports advanced vulnerability analysis.	No system model is required. However, a defensive model that identifies the logical boundaries for data transfer and associated communication protocols is recommended. This model is shown as a high-level 5-level model (L-0 through L-4) that defines the level of connectivity permitted between levels and individual CDAs.
Cyber Security Capability Development	Not only does every element in RIPE support developing cyber security capability, but the metrics to actually measure current state as well as progress toward a desired end state.	Requires that the capability to detect, respond to, and recover from cyber attacks on CDAs is implemented, documented, and maintained. RG 5.71, if fully implemented, is supposed ensure cyber security capability, but there is little guidance on how to implement a sustainable governance process or metrics that would provide adequate management thereof.
Ready-to-use Templates	Four of the eight RIPE domains are prescriptive with templates and guidance on a Training Curriculum, System Procurement, Plant Planning, as well as Policies and Standard Operating Procedures. These templates are provided and then	A template for a Cyber Security Plan provided that addresses most major elements. The guidance is intended to be general providing details on what to do with each licensee providing site specific details and flexibility in developing the "how to".

	customized in close cooperation with stakeholders.	
Information Sharing on Problems & Progress	Every aspect of RIPE, in particular vulnerability mitigation and the concept of continuous improvement, are enhanced through a process of peer-to-peer information sharing. Nonetheless, RIPE licensees may elect not to share and hence not receive any benefit therefrom.	Information sharing is not integral to the functioning of the cyber security program as outlined in RG 5.71. However, licensees are expected to report incidents and are subject to periodic inspections by the US NRC.
Cross-industry Approach	RIPE favors a cross-industry approach from the start, by focusing on providing a generic security capability baseline. Within the RIPE instruments rules are written in a way that allows for extension of generic to industry specific to application specific to version specific. Furthermore, benchmarking cross-industry is only possible when metrics are applied in a systematic and standard way. RIPE provides a means to make cross-industry benchmarking possible through objective standardized measurements of security posture.	There is no cross-industry approach within RG 5.71 and there are no metrics that would allow any meaningful comparison within the nuclear industry let alone outside the nuclear industry.
<b>RIPE Domains</b>		
System Population Characteristics	Detailed equipment and instrument list (cyber system inventory), manifested as a database, stores information on hardware systems, the software running on those systems, network association, and configuration details.	Identify and document plant systems, equipment, communication systems, and networks that are associated with safety, important-to-safety, security, and emergency preparedness (SSEP) functions, as well as the support systems associated with SSEP functions.
Network Architecture	A network architecture model, manifested as a set of diagrams with accompanying detail information for reference, identifies the connectivity options for specific endpoints and groups of endpoints. It identifies which network-connected systems can talk to which other network-connected systems.	The cyber security defensive model is deployed using a network architecture portrayed by a series of increasing defensive levels and incorporates a defense-in-depth strategy.
Component Interaction	Process flow diagrams with accompanying detail information, identifies the interfaces of digital components. For interfaces that have dedicated communication counterparts, such association is identified. Interfaces extend to non-IP networks, fieldbus, RS-232, and proprietary.	Requires restricting and controlling data flows. Validation includes the physical and logical location of each CDA, direct and indirect connectivity pathways to and from the CDA, interdependencies of the CDA, and to evaluate the effectiveness of any existing security controls and the location of the CDA in the defensive architecture.
Workforce Roles and Responsibilities	Workforce records of personnel. Identities, affiliation (staff or contractor), role-based physical and logical access and execution privileges, applicable policies and SOPs, and competence of all individuals that legitimately interact with industrial control and safety systems or process IT equipment.	Develop and implement a cyber security program that includes policies and procedures that describe the overall security goals, objectives, practices, and roles and responsibilities within the organization and, with high assurance, confirm that the cyber security program is properly established and maintained.

<p>Workforce Skills and Competence Development</p>	<p>Training curriculum and records of operations and maintenance personnel is a requirement that documents staff members and contractors' ability to perform their interactions with industrial control systems professionally and meet the provisions of policies and SOPs.</p>	<p>Individuals are trained to a level of cyber security knowledge appropriate to their assigned responsibilities in order to provide high assurance that these individuals are able to perform their job functions properly.</p>
<p>Procedural Guidance</p>	<p>Standard operating procedures used by operations and maintenance personnel for cyber, manifested as written documents, structure the activities that comprise legitimate and appropriate interaction with plant floor systems.</p>	<p>Develop and implement a cyber security program that includes policies and procedures that describe the overall security goals, objectives, practices, and roles and responsibilities within the organization and, with high assurance, confirm that the cyber security program is properly established and maintained.</p>
<p>Deliberate Design and Configuration Change</p>	<p>Plant planning and change management procedures for cyber on the topology and architecture of process networks, configuration of essential infrastructure services, authorized remote access options and products, or proper configuration and usage of virtualization technology.</p>	<p>Document the configuration management policy as a part of the configuration management plan and include hardware configurations, software configurations, and access permissions. Changes to hardware or software are documented and accessed in accordance with existing policies and implementing procedures.</p>
<p>System Acquisition</p>	<p>System procurement guidelines specifying physical and functional system attributes and properties that industrial control and safety systems, industrial network gear, and process IT systems must have in order to meet an organization's quality criteria.</p>	<p>A procurement policy that provides that the integrity of systems and services is maintained during the procurement process, development of procedures to facilitate and maintain the implementation of procurement policies associated with vendor security and development life cycles, and implementation of the security controls.</p>

## NEI 08-09 Cyber Security Plan for Nuclear Power Reactors

Developed by US Nuclear Energy Institute (NEI)

Overview NEI 08-09 is NEI’s alternative to US NRC’s RG 5.71 and provides one possible way to implement the requirements set forth in 10 CFR 73.54 which requires licensees to provide high assurance against cyber attacks.

Applies to US nuclear power plants

Hyperlink <http://pbadupws.nrc.gov/docs/ML1011/ML101180437.pdf>

	RIPE	NEI 08-09
<b>RIPE Functions</b>		
Governance	A continuous process that determines the accuracy and completeness of system documentation, and measures and enforces compliance to procedural directives periodically.	Develop, review (1-year cycle) and update a formal, documented security planning, assessment and authorization policy that describes the purpose, scope, roles, responsibilities, management commitments, and coordination and implementation of a cyber security program.
Metrics	<p>Metrics used to measure completeness, and one of the following for each of the eight RIPE domains:</p> <ul style="list-style-type: none"> <li>• accuracy,</li> <li>• compliance, or</li> <li>• conformity.</li> </ul> <p>RIPE also provides metrics for measuring RIPE documentation, policies, as well as an overall index of cyber security capability.</p>	<p>No programmatic level metrics, but recommends:</p> <ul style="list-style-type: none"> <li>• Measuring the cyber incident response capability within the organization</li> <li>• Measuring vulnerability impact</li> <li>• Developer security metrics for defect tracking within the code</li> </ul>
Structural & Behavioral System Model	Developing a detailed structural and behavioral ICS model is essential to complete system understanding. Using the information from the system inventory, network architecture diagrams, and dataflow diagrams, a detailed structural and behavioral model is developed which supports advanced vulnerability analysis.	No system model is required. However, a defensive model that identifies the logical boundaries for data transfer and associated communication protocols is recommended. This model is shown as a high-level 5-level model (L-0 through L-4) that defines the level of connectivity permitted between levels and individual CDAs.
Cyber Security Capability Development	Not only does every element in RIPE support developing cyber security capability, but the metrics to actually measure current state as well as progress toward a desired end state.	Requires that the capability to detect, respond to, and recover from cyber attacks on CDAs is implemented, documented, and maintained. NEI 08-09, if fully implemented consistent with RG 5.71, is supposed ensure cyber security capability, but there is little guidance on how to implement a sustainable governance process or metrics that would provide adequate management thereof.
Ready-to-use Templates	Four of the eight RIPE domains are prescriptive with templates and guidance on a Training Curriculum, System Procurement, Plant Planning, as well as Policies and Standard Operating Procedures. These templates are provided and then	The primary content of NEI 08-09 is a template for a Cyber Security Plan that addresses most major elements and essentially mirrors NRC’s RG 5.71. The plan template is intended to provide details on what to do with each licensee providing site specific details and flexibility in developing

	customized in close cooperation with stakeholders.	the "how to".
Information Sharing on Problems & Progress	Every aspect of RIPE, in particular vulnerability mitigation and the concept of continuous improvement, are enhanced through a process of peer-to-peer information sharing. Nonetheless, RIPE licensees may elect not to share and hence not receive any benefit therefrom.	Information sharing is not integral to the functioning of the cyber security program as outlined in NEI 08-09. However, licensees are expected to report incidents and are subject to periodic inspections by the US NRC.
Cross-industry Approach	RIPE favors a cross-industry approach from the start, by focusing on providing a generic security capability baseline. Within the RIPE instruments rules are written in a way that allows for extension of generic to industry specific to application specific to version specific. Furthermore, benchmarking cross-industry is only possible when metrics are applied in a systematic and standard way. RIPE provides a means to make cross-industry benchmarking possible through objective standardized measurements of security posture.	There is no cross-industry approach within NEI 08-09 and there are no metrics that would allow any meaningful comparison within the nuclear industry let alone outside the nuclear industry.
<b>RIPE Domains</b>		
System Population Characteristics	Detailed equipment and instrument list (cyber system inventory), manifested as a database, stores information on hardware systems, the software running on those systems, network association, and configuration details.	Identify and document plant systems, equipment, communication systems, and networks that are associated with safety, important-to-safety, security, and emergency preparedness (SSEP) functions, as well as the support systems associated with SSEP functions.
Network Architecture	A network architecture model, manifested as a set of diagrams with accompanying detail information for reference, identifies the connectivity options for specific endpoints and groups of endpoints. It identifies which network-connected systems can talk to which other network-connected systems.	The cyber security defensive model is deployed using a network architecture portrayed by a series of increasing defensive levels and incorporates a defense-in-depth strategy.
Component Interaction	Process flow diagrams with accompanying detail information, identifies the interfaces of digital components. For interfaces that have dedicated communication counterparts, such association is identified. Interfaces extend to non-IP networks, fieldbus, RS-232, and proprietary.	Requires restricting and controlling data flows. Validation includes the physical and logical location of each CDA, direct and indirect connectivity pathways to and from the CDA, interdependencies of the CDA, and to evaluate the effectiveness of any existing security controls and the location of the CDA in the defensive architecture.
Workforce Roles and Responsibilities	Workforce records of personnel. Identities, affiliation (staff or contractor), role-based physical and logical access and execution privileges, applicable policies and SOPs, and competence of all individuals that legitimately interact with industrial control and safety systems or process IT equipment.	Develop and implement a cyber security program that includes policies and procedures that describe the overall security goals, objectives, practices, and roles and responsibilities within the organization and, with high assurance, confirm that the cyber security program is properly established and maintained.

<p>Workforce Skills and Competence Development</p>	<p>Training curriculum and records of operations and maintenance personnel is a requirement that documents staff members and contractors' ability to perform their interactions with industrial control systems professionally and meet the provisions of policies and SOPs.</p>	<p>Individuals are trained to a level of cyber security knowledge appropriate to their assigned responsibilities in order to provide high assurance that these individuals are able to perform their job functions properly.</p>
<p>Procedural Guidance</p>	<p>Standard operating procedures used by operations and maintenance personnel for cyber, manifested as written documents, structure the activities that comprise legitimate and appropriate interaction with plant floor systems.</p>	<p>Develop and implement a cyber security program that includes policies and procedures that describe the overall security goals, objectives, practices, and roles and responsibilities within the organization and, with high assurance, confirm that the cyber security program is properly established and maintained.</p>
<p>Deliberate Design and Configuration Change</p>	<p>Plant planning and change management procedures for cyber on the topology and architecture of process networks, configuration of essential infrastructure services, authorized remote access options and products, or proper configuration and usage of virtualization technology.</p>	<p>Document the configuration management policy as a part of the configuration management plan and include hardware configurations, software configurations, and access permissions. Changes to hardware or software are documented and accessed in accordance with existing policies and implementing procedures.</p>
<p>System Acquisition</p>	<p>System procurement guidelines specifying physical and functional system attributes and properties that industrial control and safety systems, industrial network gear, and process IT systems must have in order to meet an organization's quality criteria.</p>	<p>Recommends that contracts specify cyber security requirements for vendors and contractors and these are applied while on site or used during procurement.</p>

## ISO 27000

Developed by	International Standards Organization (ISO)
Overview	International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art.
Applies to	Applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).
Hyperlink	<a href="http://www.iso.org/iso/catalogue_detail?csnumber=63411">http://www.iso.org/iso/catalogue_detail?csnumber=63411</a>

	RIPE	ISO 27000 (ISMS Family of Standards)
<b>RIPE Functions</b>		
Governance	A continuous process that determines the accuracy and completeness of system documentation, and measures and enforces compliance to procedural directives periodically.	An information security management system (ISMS) that includes organizational structure, policies, planning, responsibilities, practices, procedures, processes and resources. Based on the Plan-Do-Check-Act process, defines information security in terms of confidentiality, availability and integrity. (ISO 27014 – Governance)
Metrics	<p>Metrics used to measure completeness, and one of the following for each of the eight RIPE domains:</p> <ul style="list-style-type: none"> <li>• accuracy,</li> <li>• compliance, or</li> <li>• conformity.</li> </ul> <p>RIPE also provides metrics for measuring RIPE documentation, policies, as well as an overall index of cyber security capability.</p>	<p>Provides guidance on the development and use of measurements in order to assess the effectiveness of ISMS, control objectives, and controls used to implement and manage information security, as specified in ISO 27001. (ISO 27004 – Measurement)</p> <p>However, currently, there is no generally accepted means to measure the effectiveness of cyber security programs, objectives, or controls. For example, was the control effective or did the hackers just decide to take a holiday?</p>
Structural & Behavioral System Model	Developing a detailed structural and behavioral ICS model is essential to complete system understanding. Using the information from the system inventory, network architecture diagrams, and dataflow diagrams, a detailed structural and behavioral model is developed which supports advanced vulnerability analysis.	There is no requirement for critical infrastructure asset owners to develop a structural and behavioral system model.
Cyber Security Capability Development	Not only does every element in RIPE support developing cyber security capability as the first order of business, but the metrics to actually measure current state and progress toward a desired end state.	There is an unstated assumption that those who want to adopt ISO 27000 already have the cyber security capability to establish, implement, maintain and continually improve an information security management system.
Ready-to-use Templates	Four of the eight RIPE domains are prescriptive with templates and guidance on a Training Curriculum, System Procurement, Plant Planning, as well as Policies and Standard Operating Procedures. These	Templates and checklists are available from third party suppliers. However, there is no requirement and therefore no templates available for critical ICS program elements such as architecture or data flow diagrams.

	templates are provided and then customized in close cooperation with stakeholders.	
Information Sharing on Problems & Progress	Every aspect of RIPE, in particular vulnerability mitigation and the concept of continuous improvement, are enhanced through a process of peer-to-peer information sharing. Nonetheless, RIPE licensees may elect not to share and hence not receive any benefit therefrom.	Information sharing is not integral to the functioning of ISO 27000. However, the information gained through the implementation and operation of an ISO 27000 based cyber security program will do little to identify and mitigate ICS vulnerabilities.
Cross-industry Approach	RIPE favors a cross-industry approach from the start, by focusing on providing a generic security capability baseline. Within the RIPE instruments rules are written in a way that allows for extension of generic to industry specific to application specific to version specific. Furthermore, benchmarking cross-industry is only possible when metrics are applied in a systematic and standard way. RIPE provides a means to make cross-industry benchmarking possible through objective standardized measurements of security posture.	Benchmarking cross-industry is only possible when a cyber security program and metrics are applied in a systematic and standard way. Cross-industry ISO 27000 compliance comparisons do little to enlighten ICS owners because of scant coverage of ICS related cyber security issues.
<b>RIPE Domains</b>		
System Population Characteristics	Detailed equipment and instrument list (cyber system inventory), manifested as a database, stores information on hardware systems, the software running on those systems, network association, and configuration details.	Asset owners are required to identify information assets and determine their value to support the risk analysis.
Network Architecture	A network architecture model, manifested as a set of diagrams with accompanying detail information for reference, identifies the connectivity options for specific endpoints and groups of endpoints. It identifies which network-connected systems can talk to which other network-connected systems.	Recognizes that information, and related processes, systems, networks and people are important assets for achieving organization objectives.
Component Interaction	Process flow diagrams with accompanying detail information, identifies the interfaces of digital components. For interfaces that have dedicated communication counterparts, such association is identified. Interfaces extend to non-IP networks, fieldbus, RS-232, and proprietary.	Recognizes that information, and related processes, systems, networks and people are important assets for achieving organization objectives.
Workforce Roles and Responsibilities	Workforce records of personnel. Identities, affiliation (staff or contractor), role-based physical and logical access and execution privileges, applicable policies and SOPs, and competence of all individuals that legitimately interact with industrial control and safety	The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

	systems or process IT equipment.	
Workforce Skills and Competence Development	Training curriculum and records of operations and maintenance personnel is a requirement that documents staff members and contractors' ability to perform their interactions with industrial control systems professionally and meet the provisions of policies and SOPs.	Requires an effective information security awareness, training and education program, informing all employees and other relevant parties of their information security obligations set forth in the information security policies, standards and motivates them to act accordingly.
Procedural Guidance	Standard operating procedures used by operations and maintenance personnel for cyber, manifested as written documents, structure the activities that comprise legitimate and appropriate interaction with plant floor systems.	The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.
Deliberate Design and Configuration Change	Plant planning and change management procedures for cyber on the topology and architecture of process networks, configuration of essential infrastructure services, authorized remote access options and products, or proper configuration and usage of virtualization technology.	The term information security is generally based on information being considered as an asset which has a value requiring appropriate protection against the loss of availability, confidentiality and integrity.  Note: ISO 27000 defines the accuracy and completeness of assets as integral to the asset's integrity.
System Acquisition	System procurement guidelines specifying physical and functional system attributes and properties that industrial control and safety systems, industrial network gear, and process IT systems must have in order to meet an organization's quality criteria.	No specific procurement guidance provided. However, the principles of information security could be applied to any organizational activity to include procurement to ensure protection against the loss of availability, confidentiality and integrity.

## WIB Process Control Domain Vendor Requirements

Developed by	International Instrument Users Association
Overview	Provide relevant information and tools which: allow members optimally to specify, select, operate and maintain quality industrial measurement, control and automation instruments and systems, which are safe, reliable and economical; stimulate manufacturers to develop and make available automation and process control technology and products which are fit-for-purpose.
Applies to	Process industries
Hyperlink	<a href="http://www.wib.nl/">http://www.wib.nl/</a>

	RIPE	WIB
<b>RIPE Functions</b>		
Governance	A continuous process that determines the accuracy and completeness of system documentation, and measures and enforces compliance to procedural directives periodically.	The WIB is not an overall framework for the implementation and governance of a cyber security program. It is focused on the process of procuring certified secure systems or components. However, many of the practices could be applied more broadly to drive a higher level of robustness and security across the plant.
Metrics	<p>Metrics used to measure completeness, and one of the following for each of the eight RIPE domains:</p> <ul style="list-style-type: none"> <li>• accuracy,</li> <li>• compliance, or</li> <li>• conformity.</li> </ul> <p>RIPE also provides metrics for measuring RIPE documentation, policies, as well as an overall index of cyber security capability.</p>	Metrics are not specified per se nor are they programmatic in nature. However, the functional requirements of WIB ensure empirical data, in the form of measurements or quantitative analysis, are used to verify compliance.
Structural & Behavioral System Model	Developing a detailed structural and behavioral ICS model is essential to complete system understanding. Using the information from the system inventory, network architecture diagrams, and dataflow diagrams, a detailed structural and behavioral model is developed which supports advanced vulnerability analysis.	Provides a data acquisition and control reference architecture as an example. However, the standard does not suggest nor require that that asset owners actually construct a detailed model of their own network.
Cyber Security Capability Development	Not only does every element in RIPE support developing cyber security capability, but the metrics to actually measure current state as well as progress toward a desired end state.	The WIB will help to develop a capability for procuring more secure systems and components, but does not address the overall cyber security capability for the organization.
Ready-to-use Templates	Four of the eight RIPE domains are prescriptive with templates and guidance on a Training Curriculum, System Procurement, Plant Planning, as well as Policies and Standard Operating Procedures. These templates are provided and then	Does not contain user templates, but principals are encouraged to supplement with detailed practices.

	customized in close cooperation with stakeholders.	
Information Sharing on Problems & Progress	Every aspect of RIPE, in particular vulnerability mitigation and the concept of continuous improvement, are enhanced through a process of peer-to-peer information sharing. Nonetheless, RIPE licensees may elect not to share and hence not receive any benefit therefrom.	Information sharing is not required nor suggested as a best practice.
Cross-industry Approach	RIPE favors a cross-industry approach from the start, by focusing on providing a generic security capability baseline. Within the RIPE instruments rules are written in a way that allows for extension of generic to industry specific to application specific to version specific. Furthermore, benchmarking cross-industry is only possible when metrics are applied in a systematic and standard way. RIPE provides a means to make cross-industry benchmarking possible through objective standardized measurements of security posture.	WIB suggests that the results of the first risk assessment serve as a benchmark. However, because of the inherent variability in risk assessment results, cross-industry comparisons would be of little value.
<b>RIPE Domains</b>		
System Population Characteristics	Detailed equipment and instrument list (cyber system inventory), manifested as a database, stores information on hardware systems, the software running on those systems, network association, and configuration details.	Requires detailed characteristics and configuration details to achieve certification before procurement of any given system, component or device. Although the WIB certification process is applied to a single device or component, it could be applied plant-wide.
Network Architecture	A network architecture model, manifested as a set of diagrams with accompanying detail information for reference, identifies the connectivity options for specific endpoints and groups of endpoints. It identifies which network-connected systems can talk to which other network-connected systems.	Provides a notional data acquisition and control (DACA) reference architecture, but is not a requirement to meet WIB as a procurement standard.
Component Interaction	Process flow diagrams with accompanying detail information, identifies the interfaces of digital components. For interfaces that have dedicated communication counterparts, such association is identified. Interfaces extend to non-IP networks, fieldbus, RS-232, and proprietary.	Provides requirements for system, components, or device interfaces, interactions, and performance characteristics.
Workforce Roles and Responsibilities	Workforce records of personnel. Identities, affiliation (staff or contractor), role-based physical and logical access and execution privileges, applicable policies and SOPs, and competence of all individuals that legitimately interact with industrial control and safety systems or process IT equipment.	Define responsibilities of the vendor and then focuses on the transfer of that responsibility to the asset owner at the time of commissioning.

<p>Workforce Skills and Competence Development</p>	<p>Training curriculum and records of operations and maintenance personnel is a requirement that documents staff members and contractors' ability to perform their interactions with industrial control systems professionally and meet the provisions of policies and SOPs.</p>	<p>The vendor ensures competent and skilled workforce and provides information on potential security risks and recommended mitigation procedures during commissioning security awareness training.</p>
<p>Procedural Guidance</p>	<p>Standard operating procedures used by operations and maintenance personnel for cyber, manifested as written documents, structure the activities that comprise legitimate and appropriate interaction with plant floor systems.</p>	<p>Focused on validating the vendors procedures, but the asset owner needs to develop complimentary processes internal to their own organization.</p>
<p>Deliberate Design and Configuration Change</p>	<p>Plant planning and change management procedures for cyber on the topology and architecture of process networks, configuration of essential infrastructure services, authorized remote access options and products, or proper configuration and usage of virtualization technology.</p>	<p>Focused on the configuration of the system, component, or product during the development and testing phases of acquisition process. Nonetheless, the asset owner needs to develop complimentary processes internal to their own organization.</p>
<p>System Acquisition</p>	<p>System procurement guidelines specifying physical and functional system attributes and properties that industrial control and safety systems, industrial network gear, and process IT systems must have in order to meet an organization's quality criteria.</p>	<p>The primary focus of the WIB is to assist asset owners in the acquisition of ICS/SCADA systems or components that are certified at a quantified level of robustness and security.</p>

## DOE Cybersecurity Capability Maturity Model (C2M2)

Developed by US Department of Energy (DOE)

Overview The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) was established as a result of the Administration’s efforts to improve electricity subsector cybersecurity capabilities, and to understand the cybersecurity posture of the energy sector.

Applies to Electrical power industry

Hyperlink <http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity>

	RIPE	DOE C2M2
<b>RIPE Functions</b>		
Governance	A continuous process that determines the accuracy and completeness of system documentation, and measures and enforces compliance to procedural directives periodically.	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization’s cybersecurity activities in a manner that aligns cybersecurity objectives with the organization’s strategic objectives and the risk to critical infrastructure.
Metrics	<p>Metrics used to measure completeness, and one of the following for each of the eight RIPE domains:</p> <ul style="list-style-type: none"> <li>• accuracy,</li> <li>• compliance, or</li> <li>• conformity.</li> </ul> <p>RIPE also provides metrics for measuring RIPE documentation, policies, as well as an overall index of cyber security capability.</p>	Future versions of C2M2 will include: Guidance on developing a cybersecurity performance metrics and measurement program. Currently, users are given a qualitative scale for measuring cyber security maturity.
Structural & Behavioral System Model	Developing a detailed structural and behavioral ICS model is essential to complete system understanding. Using the information from the system inventory, network architecture diagrams, and dataflow diagrams, a detailed structural and behavioral model is developed which supports advanced vulnerability analysis.	The model provided in the C2M2 is a programmatic model only. There is not suggestion or requirement to build a structural or behavioral model of the asset owner’s network. However, it is suggested that asset owners address threats and vulnerabilities, but there is no guidance on how this is done.
Cyber Security Capability Development	Not only does every element in RIPE support developing cyber security capability, but the metrics to actually measure current state as well as progress toward a desired end state.	There is an implied assumption that the adopting organization will not be able to understand or implement the C2M2 without the help of an experienced facilitator. Once this hurdle is cleared, asset owners are then provided a qualitative scale of maturity to rate their cyber security capability.
Ready-to-use Templates	Four of the eight RIPE domains are prescriptive with templates and guidance on a Training Curriculum, System Procurement, Plant Planning, as well as Policies and Standard	No templates are provided.

	Operating Procedures. These templates are provided and then customized in close cooperation with stakeholders.	
Information Sharing on Problems & Progress	Every aspect of RIPE, in particular vulnerability mitigation and the concept of continuous improvement, are enhanced through a process of peer-to-peer information sharing. Nonetheless, RIPE licensees may elect not to share and hence not receive any benefit therefrom.	Provides a framework for information sharing among utilities, as well as between utilities and the government via various organizations such as ES-ISAC and US-CERT.
Cross-industry Approach	RIPE favors a cross-industry approach from the start, by focusing on providing a generic security capability baseline. Within the RIPE instruments rules are written in a way that allows for extension of generic to industry specific to application specific to version specific. Furthermore, benchmarking cross-industry is only possible when metrics are applied in a systematic and standard way. RIPE provides a means to make cross-industry benchmarking possible through objective standardized measurements of security posture.	Although not integral to the C2M2, the framework for information sharing could provide a means to benchmark utilities. However, effective benchmarking is really only possible when a cyber security program and metrics are applied in a systematic and standard way.
<b>RIPE Domains</b>		
System Population Characteristics	Detailed equipment and instrument list (cyber system inventory), manifested as a database, stores information on hardware systems, the software running on those systems, network association, and configuration details.	An inventory of assets important to the delivery of the function that records important information, such as software version, physical location, asset owner, and priority. For example, a robust asset inventory can identify the deployment location of software that requires patching, SCADA set points, historian, or state estimations.
Network Architecture	A network architecture model, manifested as a set of diagrams with accompanying detail information for reference, identifies the connectivity options for specific endpoints and groups of endpoints. It identifies which network-connected systems can talk to which other network-connected systems.	A cybersecurity architecture describes the structure and behavior of an enterprise's security processes, cybersecurity systems, personnel, and subordinate organizations and aligns them with the organization's mission and strategic plans. An important element of the cybersecurity architecture is effective isolation of IT systems from OT systems.
Component Interaction	Process flow diagrams with accompanying detail information, identifies the interfaces of digital components. For interfaces that have dedicated communication counterparts, such association is identified. Interfaces extend to non-IP networks, fieldbus, RS-232, and proprietary.	No similar requirement. However, some of the suggested inventory attributes could include information such as process flow and various ICS interfaces.
Workforce Roles and Responsibilities	Workforce records of personnel. Identities, affiliation (staff or contractor), role-based physical and logical access and execution privileges, applicable policies and SOPs, and competence of all	Ensure adequacy and redundancy of coverage for specific workforce roles with significant cybersecurity responsibilities. Cybersecurity responsibilities are not restricted to traditional IT roles; for example, some operations engineers may have

	individuals that legitimately interact with industrial control and safety systems or process IT equipment.	cybersecurity responsibilities.
Workforce Skills and Competence Development	Training curriculum and records of operations and maintenance personnel is a requirement that documents staff members and contractors' ability to perform their interactions with industrial control systems professionally and meet the provisions of policies and SOPs.	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives. New personnel (and contractors) should receive security awareness training.
Procedural Guidance	Standard operating procedures used by operations and maintenance personnel for cyber, manifested as written documents, structure the activities that comprise legitimate and appropriate interaction with plant floor systems.	Each of the model's 10 domains is a structured set of cybersecurity practices and three of those domains; Threat and Vulnerability Management, Event and Incident Response, and Continuity of Operations Workforce Management specifically call for procedure to be developed and maintained.
Deliberate Design and Configuration Change	Plant planning and change management procedures for cyber on the topology and architecture of process networks, configuration of essential infrastructure services, authorized remote access options and products, or proper configuration and usage of virtualization technology.	Managing changes to assets includes analyzing requested changes to ensure they do not introduce unacceptable vulnerabilities into the operating environment, ensuring all changes follow the change management process, and identifying unauthorized changes. Change control applies to the entire asset lifecycle.
System Acquisition	System procurement guidelines specifying physical and functional system attributes and properties that industrial control and safety systems, industrial network gear, and process IT systems must have in order to meet an organization's quality criteria.	Procurement activities are constrained by plan or policy to include cybersecurity requirements. Agreements with suppliers require notification of vulnerability-inducing product defects throughout the lifecycle of delivered products. Acceptance testing includes cybersecurity requirements and sources are monitored to avoid supply chain threats.

## NIST Cyber Security Framework (CSF)

- Developed by US National Institute of Standards and Technology (NIST)
- Overview In response to Executive Order 13636, NIST developed the CSF that focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization’s risk management processes.
- Applies to Critical infrastructure
- Hyperlink <http://www.nist.gov/cyberframework/>

	RIPE	NIST CSF
<b>RIPE Functions</b>		
Governance	A continuous process that determines the accuracy and completeness of system documentation, and measures and enforces compliance to procedural directives periodically.	Organizational information security policy is established, roles & responsibility are coordinated and aligned, legal and regulatory requirements including privacy and civil liberties. High-level statements followed by pointers to: ISA, COBIT, ISO/IEC, and other NIST guidance.
Metrics	<p>Metrics used to measure completeness, and one of the following for each of the eight RIPE domains:</p> <ul style="list-style-type: none"> <li>• accuracy,</li> <li>• compliance, or</li> <li>• conformity.</li> </ul> <p>RIPE also provides metrics for measuring RIPE documentation, policies, as well as an overall index of cyber security capability.</p>	No cyber security programmatic metrics are suggested within the NIST CSF. The only mention of metrics is related to the lack of standardization and supporting privacy metrics to assess the effectiveness of methods to protect Personally Identifiable Information (PII).
Structural & Behavioral System Model	Developing a detailed structural and behavioral ICS model is essential to complete system understanding. Using the information from the system inventory, network architecture diagrams, and dataflow diagrams, a detailed structural and behavioral model is developed which supports advanced vulnerability analysis.	No structural or behavioral ICS system model is required or suggested as an important step in system understanding or vulnerability analysis.
Cyber Security Capability Development	Not only does every element in RIPE support developing cyber security capability, but the metrics to actually measure current state as well as progress toward a desired end state.	There is an assumption that an organization has the needed capability to interpret and implement the NIST CSF.
Ready-to-use Templates	Four of the eight RIPE domains are prescriptive with templates and guidance on a Training Curriculum, System Procurement, Plant Planning, as well as Policies and Standard Operating Procedures. These templates are provided and then customized in close cooperation with stakeholders.	The NIST CSF does not contain any end user templates that would facilitate implementation.
Information	Every aspect of RIPE, in particular	Recommends that voluntary information

Sharing on Problems & Progress	vulnerability mitigation and the concept of continuous improvement, are enhanced through a process of peer-to-peer information sharing. Nonetheless, RIPE licensees may elect not to share and hence not receive any benefit therefrom.	sharing should occur with external stakeholders, such as the various Information Sharing and Analysis Centers (ISACs) to achieve broader cybersecurity situational awareness.
Cross-industry Approach	RIPE favors a cross-industry approach from the start, by focusing on providing a generic security capability baseline. Within the RIPE instruments rules are written in a way that allows for extension of generic to industry specific to application specific to version specific. Furthermore, benchmarking cross-industry is only possible when metrics are applied in a systematic and standard way. RIPE provides a means to make cross-industry benchmarking possible through objective standardized measurements of security posture.	There is no cross-industry approach within the NIST CSF nor are there metrics that would allow meaningful comparison within any particular industry let alone cross-industry.
<b>RIPE Domains</b>		
System Population Characteristics	Detailed equipment and instrument list (cyber system inventory), manifested as a database, stores information on hardware systems, the software running on those systems, network association, and configuration details.	Physical devices and systems within the organization are inventoried. Software platforms and applications within the organization are inventoried. External information systems are mapped and catalogued. High-level statements followed by pointers to standards such as ISA, COBIT, ISO/IEC, SANS and NIST.
Network Architecture	A network architecture model, manifested as a set of diagrams with accompanying detail information for reference, identifies the connectivity options for specific endpoints and groups of endpoints. It identifies which network-connected systems can talk to which other network-connected systems.	No guidance provided in the CSF except for what may be found in the referenced standards such as ISA, COBIT, ISO/IEC, SANS and NIST.
Component Interaction	Process flow diagrams with accompanying detail information, identifies the interfaces of digital components. For interfaces that have dedicated communication counterparts, such association is identified. Interfaces extend to non-IP networks, fieldbus, RS-232, and proprietary.	The organizational communication and data flow is mapped. However, there is no guidance provided on the level of detail or just what to do with this data flow map except for what may be found in the referenced standards such as ISA, COBIT, ISO/IEC, SANS and NIST.
Workforce Roles and Responsibilities	Workforce records of personnel. Identities, affiliation (staff or contractor), role-based physical and logical access and execution privileges, applicable policies and SOPs, and competence of all individuals that legitimately interact with industrial control and safety systems or process IT equipment.	Workforce roles and responsibilities for business functions, including cybersecurity, are established. Access to information resources and associated facilities are limited to authorized users, processes or devices, and to authorized activities and transactions. Detailed guidance is provided by ISA, COBIT, ISO/IEC, SANS and NIST.

<p>Workforce Skills and Competence Development</p>	<p>Training curriculum and records of operations and maintenance personnel is a requirement that documents staff members and contractors' ability to perform their interactions with industrial control systems professionally and meet the provisions of policies and SOPs.</p>	<p>The organization's personnel and partners are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. Detailed guidance is provided by ISA, COBIT, ISO/IEC, SANS and NIST.</p>
<p>Procedural Guidance</p>	<p>Standard operating procedures used by operations and maintenance personnel for cyber, manifested as written documents, structure the activities that comprise legitimate and appropriate interaction with plant floor systems.</p>	<p>The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. Detailed guidance provided in ISA, COBIT, ISO/IEC, SANS and NIST.</p>
<p>Deliberate Design and Configuration Change</p>	<p>Plant planning and change management procedures for cyber on the topology and architecture of process networks, configuration of essential infrastructure services, authorized remote access options and products, or proper configuration and usage of virtualization technology.</p>	<p>A baseline configuration of information technology/operational technology systems is created and configuration change control processes are in place. Users are expected to find detailed guidance in ISA, COBIT, ISO/IEC, SANS and NIST.</p>
<p>System Acquisition</p>	<p>System procurement guidelines specifying physical and functional system attributes and properties that industrial control and safety systems, industrial network gear, and process IT systems must have in order to meet an organization's quality criteria.</p>	<p>No guidance provided in the CSF except for what may be found in the other referenced standards such as ISA, COBIT, ISO/IEC, SANS and NIST.</p>