in effecting change, Attributes that maximize benefit relative to the utility's key goals, or Attributes that minimize risks (e.g., fines, penalties, lawsuits, poor public perception).

The choice to embark on improvements in one or more areas is up to the judgment of utility managers, and may also involve consideration of resources (staff and financial), leadership support, and other competing activities. Applying strategic business planning, measurement, and other Keys to Management Success is very important for moving each Attribute over time to the "high-achievement" quadrants.

# V. Getting to Work: Implementation of Effective Utility Management

This section focuses on the specific steps that utilities are encouraged to go through to implement Effective Utility Management. The section includes a description of each element of the Effective Utility Management (EUM) cycle, and explains how utilities can take the results of their self-assessment, identify and implement effective practices, measure progress in priority Attribute areas, and do this through an improvement plan.

The EUM self-assessment (see page 11 for more information) serves as a comprehensive starting point for utilities, and the EUM cycle reflects how a utility's self-assessment results

can build into a continual improvement management process. **Continual improvement** is one of the five Keys to Management Success for Effective Utility Management, and it operates throughout and supports the entire EUM cycle. The water sector is a rapidly evolving world, and utilities must stay abreast of new technologies, changes in the workforce, transforming customer needs, and much more. To adapt to these shifts, an effective utility must continually assess its performance and priorities, update its strategic plan, and make adjustments where necessary.

Two other Keys are reflected directly in the EUM cycle, **strategic business planning** and **measurement**; these are explained in greater detail later in this section. The two remaining Keys are also important to supporting all aspects of the EUM cycle: **leadership** and **knowledge management**. Leadership can exist at any level of a utility's organizational structure, and can encourage and enable active participation in an Effective Utility Management culture. Knowledge management supports the critical information and operating needs of each step of the cycle of Effective Utility Management. All five of the Keys to Management Success (see page 8 for more information) are integral to Effective Utility Management, and they work in tandem with the Ten Attributes (see page 4 for more information) to support successful utilities.

Beginning with the **self-assessment** exercise in **Section IV**, the EUM cycle is a self-reinforcing progression of assessment, planning, implementation, measurement, and adjusting over time. Each element of the cycle is described below.
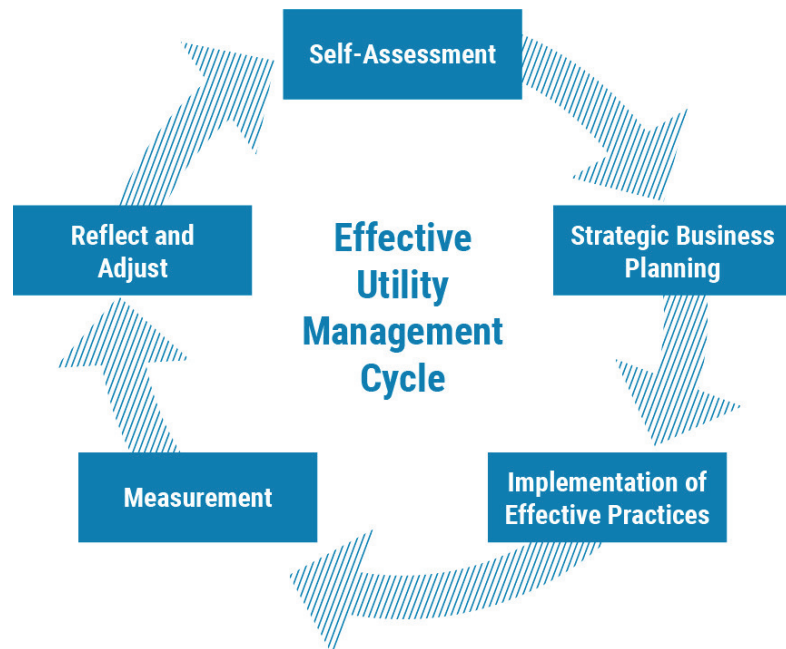
Strategic Business Planning

Following completion of the self-assessment, utilities will now have a holistic picture of their current performance and priorities for the future relative to the Ten Attributes. Using these results as a starting point, a utility can begin to move through a strategic business planning process. Strategic business planning provides a framework for decision making and planning for the future. A strategic business plan could include, or be complemented by, an asset management plan and a financial plan for the utility.

Implementation of Effective Practices

After the utility has determined its priority Attribute areas for improvement and established a vision, goals, and objectives for the future through its strategic business plan, it is time to identify and implement effective practices linked to the Attributes in support of these objectives. Effective practices can also be identified in many ways: through learning activities (e.g., conferences, training events, webinars), through interactions and benchmarking activities with other utilities, and through resources created specifically to guide utilities in this area.

Two key resources to help utilities link the Attributes to specific practices are *Moving Toward Sustainability: Sustainable and Effective Practices for Creating Your Water Sector Roadmap,* developed by EPA with extensive input from water sector leaders, and *Performance Benchmarking for Effectively Managed Utilities* (Water Research Foundation), also prepared with extensive utility participation. Both are available at www.WaterEUM.org.

Measurement

To gauge performance and progress on the utility's strategic plan and practice implementation, the next step in the cycle is to establish performance measures relative to key activities. The adage of "you can't improve what you don't measure" applies here. Measurement is a key focus of this *Primer*, with approaches and example measures that utilities can implement addressed in greater depth later in this section and in **Appendix C**.
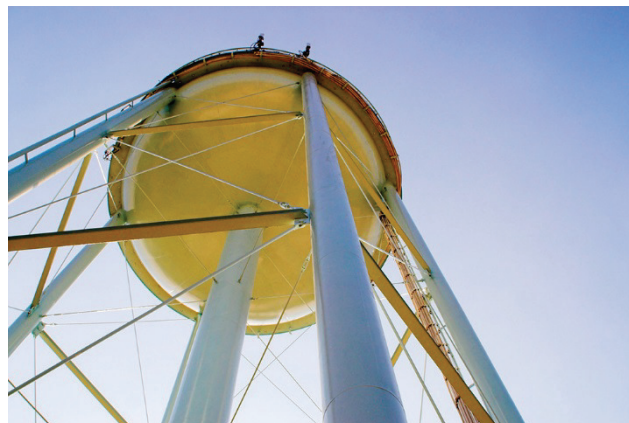
Reflect and Adjust

At regular intervals, the utility should reflect on its progress toward the goals set forth in its strategic business plan and its improvement plan relative to the Attributes, and determine if adjustments in course are needed, accounting for any changes in the utility's operating context.

Utilities can implement the cycle of Effective Utility Management in a variety of ways. It can be integrated into processes already in place as a part of the utility's operations and management, incorporated into a long-term planning process, or undertaken independently. A short guide for creating an improvement plan based on the self-assessment results follows at the end of this section.

Measuring Performance

Measuring performance is one of the keys to utility management success. This section of the *Primer* provides ideas about how to approach measurement and then offers measures for each Attribute to help utilities understand their current status and measure their progress.

Approaching Measurement

There are two general approaches to performance measurement: internal and external benchmarking. This *Primer* focuses on internal performance measurement. Internal performance measurement focuses on evaluating current internal utility performance status and trends. A robust measurement system will be built around a combination of leading, lagging, and coincidental performance indicators.

- **Leading indicators** provide an indication of the future state of a performance parameter of keen interest to the utility – for example an increase in near misses relative to safety violations can foretell of an increased risk of workplace injuries. Leading indicators provide a utility with the diagnostic ability to proactively manage for its desired performance outcomes. *Leading indicators drive preventative actions.*
- **Lagging indicators** typically reflect a performance parameter of keen interest to a utility (such as compliance rate or water quality conditions) while, at the same time providing performance information that can only be reacted to, making it sometimes challenging to proactively adjust operations before performance moves into an unacceptable range. These indicators, however, are critical to an overall measurement system as they typically focus on key performance outcomes that the utility, by necessity, must document (e.g., compliance with permit limits). *Lagging indicators drive immediate, corrective actions that could have been prevented by using leading and coincidental indicators.*

LEADING, LAGGING, AND COINCIDENTAL INDICATORS

A real-life example of applying indicators when analyzing body mass:

Lagging: At the end of the day, stepping on a scale and recording your weight.

Leading: Tracking the number of calories consumed and the number of calories expended through exercise.

Coincidental: Analyzing the two measurements, calories consumed and calories expended holistically. This will allow you to predict that if calories go up and exercise goes down, you can expect an increase in weight.

- **Coincidental indicators** are a form of leading indicator that draws on the behavior of two or more parameters to signal the future state of a key performance parameter (such as phosphorus discharge concentration). These indicators are important to both proactive management of key performance outcomes, but also to conducting root cause analysis when key performance outcomes vary outside of desirable ranges. *Coincidental indicators drive proactive process control actions.*

Benchmarking is the overt comparison of similar measures or processes across organizations to identify best practices, set improvement targets, and measure progress within or sometimes across sectors. A utility may decide to engage in benchmarking for its own internal purposes or in a coordinated fashion with others.

While performance measures should be tailored to the specific needs of your utility, the following guidelines can help you identify useful measures and apply them effectively.

1. Select measures that support the organization's strategic objectives, mission, and vision, as well as the ten Attributes.
2. Select the right number, level, and type of measures for your organization. Consider how measures can be integrated as a cohesive group (e.g., start with a small set of measures across broad categories and increase number and specificity over time as needed), and consider measures that can be used by different audiences within the organization.
3. Measuring performance will not necessarily require additional staff, but will require resources. Allocate adequate resources to get the effort off to a good start, and fine tune over time to balance the level of measurement effort with the benefit to the organization.
4. Develop clear, consistent definitions for each measure. Identify who is responsible for collecting the data, and how the data will be tracked and reported.
5. Engage the organization at all levels in developing, tracking, and reporting measures, but also assign someone in the organization the role of championing and coordinating the effort.
6. Set targets rationally, based on criteria such as customer expectations, improvement over previous years, industry performance, or other appropriate comparisons. Tie targets to improving performance in the Attributes.
7. Select and use measures in a positive way to improve decision making, clarify expectations, and focus attention, not just to monitor, report, and control.
8. When selecting measures, consider how they relate to one another. Look for cause-and-effect relationships; for example, how improvements in product quality could result in increased customer satisfaction.
9. Develop an effective process to evaluate and respond to results. Identify how, when, and to whom you will communicate results.
10. Incorporate the "Plan-Do-Check-Act" cycle approach into evaluating both the specific measures and the system as a whole. Regularly review the performance measurement system for opportunities to improve.

   … and remember to celebrate your measured and documented successes!

Attribute-Related Measures

The list on the following page provides examples of targeted, Attribute-related measures. Taken as a whole, the measures provide a utility with a cohesive, approachable, and generally applicable starting place for gauging progress relative to the Ten Attributes. The list, for brevity, contains measure "headlines" for each

Attribute. Utilities should also reference information in **Appendix C**, which provides further explanation and, where applicable, example calculations.

You can choose and tailor the measures to your own needs and unique, local circumstances. They are intended for your own internal use, even as certain measures (e.g., those noted as Benchmarking Performance Indicators) can support benchmarking purposes. In these cases, the measures have been selected because they are relevant to the Attributes, have been tested and are in use by utilities, are supported by reference information useful for implementation, and generally can act as a good starting point for Attribute-related progress assessment.

The measures presented are both quantitative and qualitative. Most are quantitative, focus on outcomes typically of interest to utility managers (e.g., compliance rate), and include generally applicable example calculations. The qualitative "measures" encourage active assessment of the practices in place to support effective management in each Attribute area. These are mostly "activity measures" and typically have a "yes/no" format. Like the Attributes themselves, certain measures focus on core utility operations. Several measures reflect emerging utility issues, challenges, or opportunities that have received increasing attention from a growing number of utility managers. Other measures may reflect broader interests that are worthy of consideration from a broader community perspective.

List of Attribute-Related Utility Measures

The list below includes a limited number of example measures that can be used to assess performance in each of the Attribute areas. See **Appendix C** for measure descriptions and details.

Product Quality
1. Regulatory compliance
2. Service delivery

Customer Satisfaction
1. Customer complaints
2. Customer service delivery
3. Customer satisfaction

Employee and Leadership Development
1. Employee retention and satisfaction
2. Management of core competencies
3. Workforce development

Operational Optimization
1. Resource optimization
2. Water management efficiency

Financial Viability
1. Budget management effectiveness
2. Financial procedure integrity
3. Bond ratings
4. Rate adequacy

Infrastructure Stability
1. Asset inventory
2. Asset (system) renewal/replacement
3. Water distribution/collection system integrity
4. Infrastructure planning and maintenance

Enterprise Resiliency
1. Recordable incidents of injury or illnesses
2. Insurance claims
3. Risk assessment and response preparedness
4. Ongoing operational resiliency
5. Operational resiliency under emergency conditions

Community Sustainability

1. Watershed-based infrastructure planning
2. Green infrastructure
3. Greenhouse gas emissions
4. Service affordability
5. Community economic development

Water Resource Sustainability

1. Water supply adequacy
2. Supply and demand management
3. Watershed sustainability

Stakeholder Understanding and Support

1. Stakeholder consultation
2. Stakeholder satisfaction
3. Internal benefits from stakeholder input
4. Comparative rate rank
5. Media/press coverage
6. Partnering in your community

Resources to Support Effective Utility Management Implementation

Effective Utility Management is designed as a broad framework to complement and enhance other prominent utility management initiatives currently in use. In addition to this EUM *Primer*, a wide range of resources exist across the water sector to support each step of the cycle of Effective Utility Management. The resources listed below are examples of materials that can support each step of the EUM cycle.

- **Benchmarking Performance Indicators for Water and Wastewater** (American Water Works Association)
- **Moving Toward Sustainability: Sustainable and Effective Practices for Creating Your Water Utility Roadmap** (U.S. EPA)
- **The Partnership for Clean Water** (American Water Works Association)
- **The Partnership for Safe Water** (American Water Works Association)
- **Performance Benchmarking for Effectively Managed Water Utilities** (Water Research Foundation)
- **Planning for Sustainability: A Handbook for Water and Wastewater Utilities** (U.S. EPA)
- **Resource Guide to Effective Utility Management and Lean: Improving Performance and Addressing Key Management Priorities at Water-Sector Utilities** (U.S. EPA)
- **The Water Resources Utility of the Future: A Blueprint for Action** (National Association of Clean Water Agencies, Water Environment & Reuse Foundation, and Water Environment Federation)

> THE DIAGRAM ON THE FOLLOWING PAGE IS A DEPICTION OF HOW EACH RESOURCE FROM THE LIST CAN RELATE TO THE VARIOUS STEPS IN THE CYCLE.

HOW IT FITS TOGETHER
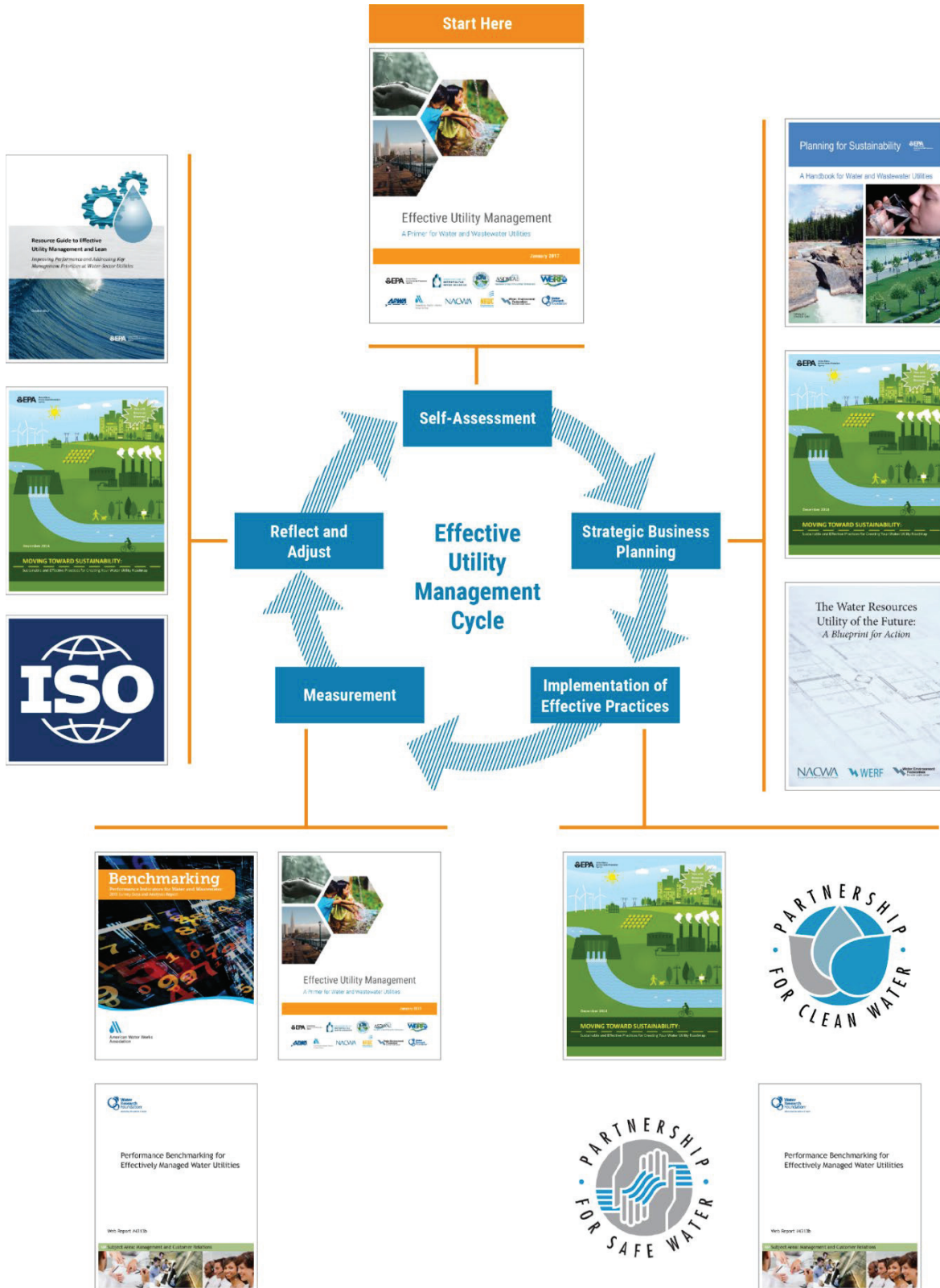
Creating an Improvement Plan

Once you have chosen to improve one or more Attributes, the next step is to develop and implement a plan for making the desired improvements. Improvement plans support the implementation of effective practices in your chosen attribute area(s). An effective improvement plan will:

|	
Set Near- and Long-term Goals	Set goals as part of the improvement plan to help define what is being worked toward. Near- and long-term goals for the utility should be linked to the strategic business plan, asset management plan, and financial plan. Goals should also be "SMART." **S – Specific:** *What exactly will be achieved?* **M – Measurable:** *Can you measure whether you are achieving the objective?* **A – Assignable:** *Can you specify who will be responsible for each segment of the objective?* **R – Realistic:** *Do you have the capacity, funding, and other resources available?* **T – Time-Based:** *What is the timeframe for achieving the objective?*
Identify Effective Practices	Each Attribute area for improvement will be supported by effective practices implemented by the utility. A substantial number of water sector resources exist that detail effective utility practices for each of the Attributes.
Identify Resources Available and Resources Needed	For each practice/activity to be implemented as part of the improvement plan, identify resources (financial, informational, staff, or other) that exist on-hand, and those that are needed, to support implementation.
Identify Challenges	For the overall improvement plan and for specific practices/activities to be implemented, identify key challenges that will need to be addressed.
Assign Roles and Responsibilities	For each improvement action, identify roles and responsibilities for bringing the implementation to completion.
Define a Timeline	Establish start date, milestones, and a completion target for each activity/improvement action.
Establish Measures	Establish at least one (or more) measure of performance for items to be implemented under the improvement plan.

VI. Utility Management Resources

As a companion resource to this Primer, the Collaborating Organizations developed an online Resource Toolbox, which offers additional information and guidance on effective utility management. The Toolbox provides a compilation of resources from the eleven Collaborating Organizations designed to help the water and wastewater utility community further improve the management of its infrastructure.

The Resource Toolbox is organized according to the Ten Attributes of Effectively Managed Water Sector Utilities and five Keys to Management Success, providing a set of resources relevant to each Attribute and Key. The Toolbox also includes information on where to find these resources.

The Resource Toolbox is located at www.WaterEUM.org.

Effective Utility Management for Small and Rural Systems

Small and rural utilities seeking to implement EUM are served by a variety of resources specifically designed for them, including the *Rural and Small Systems Guidebook to Sustainable Utility Management.* The *Guidebook* is a resource jointly developed by EPA and the United States Department of Agriculture (USDA), which adapts the Ten Attributes for use by small and rural systems.
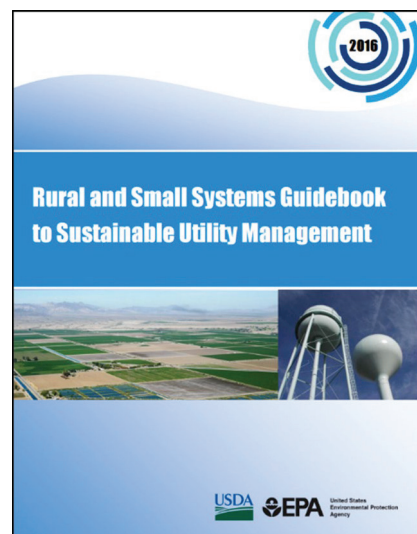
VII. For More Information

This Primer was developed through a collaborative partnership with the following groups. More information about this partnership can be found on their websites or by contacting specific individuals directly.

Association of Clean Water Administrators
Julia Anastasio
Executive Director & General Counsel
1634 I Street NW, Suite 750
Washington DC 20006
janastasio@acwa-us.org
202.756.0600
www.acwa-us.org

American Public Works Association
Anne Jackson
Director of Sustainability
1275 K Street NW, Suite 750
Washington DC 20005
ajackson@apwa.net
202.218.6750
www.apwa.net

Association of State Drinking Water Administrators
Bridget O'Grady
Policy and Legislative Affairs Manager
1401 Wilson Blvd.
Arlington, VA 22209
bogrady@asdwa.org
703.812.9505
www.asdwa.org

American Water Works Association
Cynthia Lane
Director, Engineering and Technical Services
6666 W. Quincy Ave.
Denver, CO 80235
clane@awwa.org
303.347.6176
www.awwa.org

Association of Metropolitan Water Agencies
Carolyn Peterson
Director of Communications and Public Affairs
1620 I Street, NW
Washington DC 20006
peterson@amwa.net
202.331.2820
www.amwa.net

National Association of Clean Water Agencies
Chris Hornback
Chief Technical Officer
1816 Jefferson Place, NW
Washington DC 20036
chornback@nacwa.org
202.833.9106
www.nacwa.org

National Association of Water Companies
Petra Smeltzer
Director of Government Relations
2001 L Street NW, Suite 850,
Washington DC 20036
petra@nawc.com
202.322.8089
www.nawc.org

U.S. Environmental Protection Agency
Jim Horne
Sustainability Program Manager
Office of Wastewater Management
1200 Pennsylvania Avenue, NW
Room 7111 – WJC East
Washington DC 20460
horne.james@epa.gov
202.564.0571
www.epa.gov/sustainable-water-infrastructure

Water Environment Federation
Matt Ries
Chief Technical Officer
601 Wythe Street
Alexandria, VA 22314-1994
mries@wef.org
703.684.2406
www.wef.org

Water Environment & Reuse Foundation
Allison Deines
Director of Special Projects
1199 N Fairfax St, Suite 410
Alexandria, VA 22314-1177
adeines@werf.org
571.384.2116
www.werf.org

Water Research Foundation
Linda Reekie
Research Manager
6666 West Quincy Avenue
Denver, Colorado 80235-3098
lreekie@waterrf.org
303.734.3423
www.waterrf.org

VIII. Appendix A: Key Definitions

Attribute: A basic building block of effective utility management for water sector utilities. Attributes describe characteristics or outcomes of a utility that indicate effective performance.

Benchmarking: The comparison of similar processes or measures across or within organizations and/or sectors to identify best practices, set improvement targets, and measure progress.

Continual Improvement: A systematic approach that supports ongoing efforts to improve products, services, or processes, through incremental steps over time or through "breakthrough" advances all at once.

Effective Utility Management: A comprehensive water sector utility performance assessment and management framework, endorsed by the U.S. Environmental Protection Agency and ten national water sector associations dedicated to improving products and services, increasing community support for water services, and ensuring a strong and viable utility into the future.

Gap analysis: Defining the present state of an enterprise's operations, the desired or "target" state, and the gap between them.

Knowledge Management: The multi-disciplinary process of creating, sharing, using, managing, and preserving the knowledge and information of an organization.

Life-cycle cost: The total of all internal and external costs associated with a product, process, activity, or asset throughout its entire life cycle – from raw materials acquisition to manufacture/construction/installation, operation and maintenance, recycling, and final disposal.

Performance measurement: Evaluation of current status and trends; can also include comparison of outcomes or outputs relative to goals, objectives, baselines, targets, standards, other organizations' performance or processes (typically called benchmarking), etc.

Operations and maintenance expenditure: Expenses used for day-to-day operation and maintenance of a facility.

Operating revenue: Revenue realized from the day-to-day operations of a utility.

Performance measure: A particular value or characteristic designated to measure input, output, outcome, efficiency, or effectiveness.

Source water protection: Efforts to prevent water quality degradation in streams, rivers, lakes, or underground aquifers used as public drinking water supplies.

Standard operating procedure: A prescribed set of actions to be followed routinely; a set of instructions having the force of a directive, covering those features of operations that lend themselves to a definite or standardized procedure without loss of effectiveness.

Strategic plan: An organization's process of defining its goals and strategy for achieving those goals. This often entails identifying an organization's vision, goals, objectives, and targets over a multi-year period of time, as

well as setting priorities and making decisions on allocating resources, including capital and people, to pursue the identified strategy.

Stewardship: The careful and responsible management of something entrusted to a designated person or entity's care; the responsibility to utilize its resources properly, including its people, property, and financial and natural assets.

Sustainability: The use of natural, community, and utility resources in a manner that satisfies current needs without compromising future needs or options.

Watershed health: The ability of ecosystems to provide the functions needed by plants, wildlife, and humans, including the quality and quantity of land and aquatic resources.

IX. Appendix B: Self-Assessment

Step 1: Assess Current Conditions

Assess current conditions by rating your utility's systems and approaches and <u>current level of achievement</u> for each Attribute, using a 1 (high achievement) to 5 (low achievement) scale. Consider the degree to which your current management systems effectively support each of the Attributes and their component parts. Consider all components of each Attribute and gauge your rating accordingly. Use these descriptions to guide your rating. You will note that each Attribute has several components represented by the bullet points listed for each.

Your rating can either reflect the lowest level of achievement of all of the bullet points for that Attribute (for example, if you believe that your achievement in one of the bullet points for that Attribute was "5," but another bullet point you rated as "2," your rating for achievement under that Attribute would be "5"), or an average across all of the bullet points for that Attribute. For whatever approach you choose to use when rating, make sure to be consistent in this approach across all Attributes. Mark your answers in the Step 1 column of the table on the next page.

Rating	Description
1.	Effective, systematic approach and implementation; consistently achieve goals.
2.	Workable systems in place; mostly achieve goals.
3.	Partial systems in place with moderate achievement, but could improve.
4.	Occasionally address this when specific need arises.
5.	No system for addressing this.

Step 2: Rank Importance of Attributes

Rank the importance of each Attribute to your utility, based on your utility's vision, goals, and specific needs. The ranking should reflect the interests and considerations of all stakeholders (managers, staff, customers, regulators, elected officials, community and watershed interests, and others).

There are Ten Attributes; considering long-term importance to your utility, rank the most important Attribute 1, the second most important 2, and so on. The least important Attribute would be ranked 10. Your ranking of each Attribute's importance may be influenced by current or expected challenges in that particular area, recent accomplishments in addressing these issues, or other factors. Importance ranking is likely to change over time as internal and external conditions change.

Mark your answers in the Step 2 column of the table on the next page. <u>As you fill in numbers, please note that your analysis for Step 1 (rating achievement) should be separate and independent from your analysis for Step 2 (ranking importance).</u>

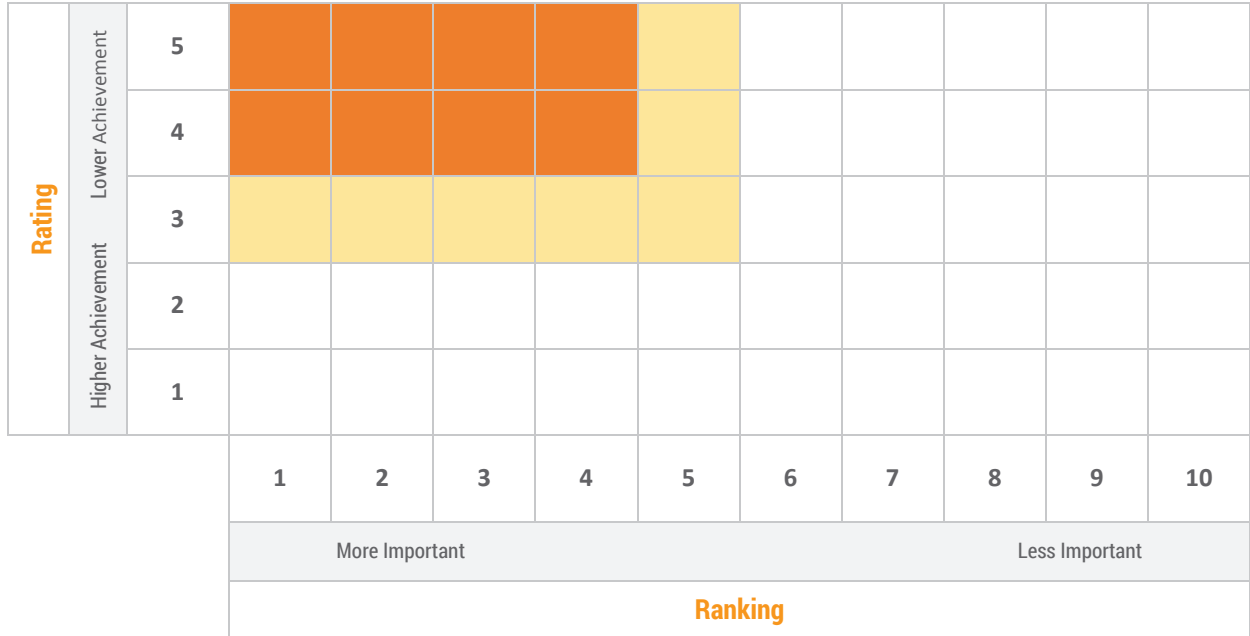| Attribute	Attribute Components	Step 1: Rate Achievement (1-5)	Step 2: Rank Importance (1-10)
Product Quality (PQ)	• Meets or exceeds regulatory and reliability requirements. • Operates consistent with customer, public health, economic, and ecological needs.		
Customer Satisfaction (CS)	• Provides reliable, responsive, and affordable services. • Receives timely customer feedback. • Is responsive to customer needs and emergencies. • Provides tailored customer service and outreach to a range of customer groups (e.g., residential, commercial, industrial, and newly emerging groups such as high-strength waste producers or power companies)		
Employee and Leadership Development (ED)	• Recruits, develops, and retains a competent, safety-focused workforce. • Is a collaborative organization dedicated to continual learning, improvement, and adaptation. • Implements procedures for institutional knowledge retention, workplace safety, and continual learning (e.g., standard operating procedures). • Invests in/provides opportunities for professional and leadership development. • Supports an integrated and well-coordinated senior leadership team.		
Operational Optimization (OO)	• Conducts ongoing performance improvements informed by performance monitoring. • Minimizes resource use and loss from day-to-day operations. • Is aware of and adopts in a timely manner operational and technology improvements, including operational technology and information technology. • Manages and utilizes data from automated and smart systems.		

Attribute	Attribute Components	Step 1: Rate Achievement (1-5)	Step 2: Rank Importance (1-10)
Financial Viability (FV)	• Understands and plans for full life-cycle cost of utility. • Effectively balances long-term debt, asset values, operations and maintenance expenditures, and operating revenues. • Sets predictable and adequate rates to support utility current needs and plans to invest in future needs, taking into account affordability and the needs of disadvantaged households when setting rates. • Understands opportunities for diversifying revenue and raising capital.		
Infrastructure Strategy and Performance (IS)	• Understands the condition of and costs associated with critical infrastructure assets. • Maintains and enhances assets over the long-term at the lowest possible life-cycle cost and acceptable risk. • Coordinates repair efforts within the community to minimize disruptions. • Plans infrastructure investments consistent with community needs, anticipated growth, system reliability goals, and with a robust set of adaptation strategies.		
Enterprise Resiliency (ER)	• Works together with staff internally and coordinate with external partners to anticipate and avoid problems. • Proactively establishes tolerance levels and effectively manages risks (including legal, regulatory, financial, environmental, safety, security, cyber, knowledge-loss, talent, and natural disaster-related). • Plans for and actively manages to maintain business continuity.		

Attribute	Attribute Components	Step 1: Rate Achievement (1-5)	Step 2: Rank Importance (1-10)
Community Sustainability (SU)	• Actively leads in promoting and organizing improvements to community and watershed health within utility and with external community partners. • Actively leads in promoting welfare within the community for disadvantaged households. • Uses operations to enhance natural environment. • Efficiently uses water and energy resources, promotes economic vitality, and engenders overall community improvement. • Maintains and enhances ecological and community sustainability including pollution prevention, watershed and source water protection.		
Water Resource Sustainability (WS)	• Ensures water availability through long-term resource supply and demand analysis, conservation, fit for purpose water reuse, integrated water resource management, watershed management and protection, and public education initiatives. • Manages operations to provide for long-term aquifer and surface water sustainability and replenishment. • Understands and plans for future water resource variability (e.g., changing weather patterns, including extreme events, such as drought and flooding).		
Stakeholder Understanding and Support (SS)	• Engenders understanding and support from oversight bodies, community and watershed interests, and regulatory bodies for service levels, rate structures, operating budgets, capital improvement programs, and risk management decisions. • Actively engages in partnerships and involves stakeholders in the decisions that will affect them. • Actively promotes an appreciation of the true value of water and water services, and water's role in the social, economic, public and environmental health of the community.		

Step 3: Graph Results

Graph each Attribute based on your rating and ranking.

Rating			1	2	3	4	5	6	7	8	9	10
	Lower Achievement	**5**										
		4										
		3										
	Higher Achievement	**2**										
		1										

|	1	2	3	4	5	6	7	8	9	10
	More Important							Less Important		

Ranking

X. Appendix C: Attribute-Related Water Utility Measures

Performance measurement is critical to effectively managing a utility. This section of the *Primer* provides detailed information on a range of measures that utilities can consider, including descriptions and example calculations and questions.

In addition to the example measures described in this section, utilities can reference a variety of resources available to the sector which provide additional specific measures for a variety of practices. Resources available to utilities include:

- **Benchmarking Performance Indicators for Water and Wastewater Utilities** (American Water Works Association)
- **Effective Utility Management Benchmarking Tool** (Water Research Foundation)

For each of the Attributes, a variety of example calculations and questions are provided in this Appendix for use by water sector utilities. This is not meant to serve as an exhaustive list, but rather a starting point for utilities as they begin to think about how performance can be measured for each Attribute.
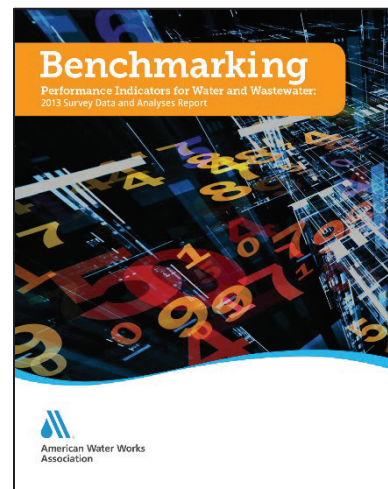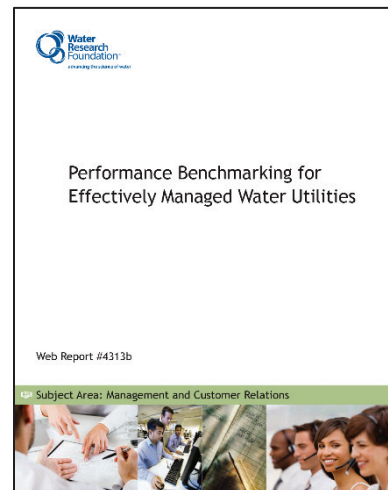
Product Quality

1. Regulatory compliance

Description: This measure assesses water product quality compliance, particularly with regard to 40 CFR Part 141 (the National Primary Drinking Water Regulations), the National Pollutant Discharge Elimination System, and any other relevant federal (Clean Water Act, Safe Drinking Water Act, etc.) or state statute/regulations and permit requirements. The scope can include the quality of all related products, including drinking water, fire suppression water, treated effluent, reused water, and biosolids (EPA 503 Regulations), as well as quality related to operating requirements such as pressure and number of sewer overflows.

Example performance measures:

- Drinking water compliance rate (percent): 100 X (number of days in full compliance for the year ÷ 365 days). *This is a Benchmarking Performance Indicator*.

- Wastewater treatment effectiveness rate (percent): 100 X (365 – total number of noncompliance days ÷ 365 days). *This is a Benchmarking Performance Indicator.*
- Number, type, and frequency of "near (compliance) misses": For example, reaching 80-95% of allowable levels of "X" during reporting period, typically per month. Tracking this type of measure could be used to improve performance in these "near miss" areas before violations occur.

2. Service delivery

Description: This measure assesses delivery of quality service based on utility-established objectives and service level targets.

Example performance measures:

- Drinking water flow and pressure (percent): 100 X [number of customers with less than (flow of "X" gallons per minute (gpm) and pressure of "Y" pounds per square inch (psi)—levels set by utility) ÷ total number of customers] (during reporting period, typically per month).
- Fire suppression water flow and pressure (percent): 100 X [hours of time when (flow of "X" gpm and pressure of "Y" psi—levels set by utility) is available for fire suppression at maximum day demand ÷ total number of hours when fire suppression water should be available at maximum day demand] (during reporting period, typically per month).
- Service interruptions (percent): 100 X (number of active account customers experiencing a service interruption of greater than 1 hour ÷ total number of customers during reporting period) (typically per month). Note: the utility may elect to measure planned and unplanned interruptions separately.
- Water quality goals met/not met: Number of days in reporting period (typically one month) where utility-defined beyond-compliance targets are met/not met.
- Sewer backups (amount and percent): Number of customers experiencing backups each year; 100 X (number of customers experiencing backups each year ÷ total number of customers).
- Sewer overflows: Number of sewer overflows per 100 miles of collection system piping, or number of sewer overflows per million gallons treated.
- Water reuse (amount and percent):
  - Amount: Amount of water supplied that is from reused/recycled sources.
  - Percent: 100 X (amount of water supplied that is from reused/recycled water ÷ total amount of water supplied).
  - Then, as desired, these amounts can be broken into recipients/applications (e.g., irrigation, agriculture, industrial processes, etc.).
- Biosolids put to beneficial use (percent): 100 X (amount of biosolids produced that are put to a beneficial use ÷ total amount of biosolids produced) (in wet tons per year).
- Percent of recovered resources that meet customer specifications or regulatory requirements: 100 X (amount of efficiently recovered material ÷ total amount of potentially recovered material).

Customer Satisfaction

1. Customer complaints

Description: This measure assesses the complaint rates experienced by the utility, with individual quantification of customer service and core utility service complaints (note that "service complaints" would not include routine service requests by customers).[1] As a "passive measure," it will not likely be numerically representative (i.e., a statistically valid customer sample group) and is a "starting point" measure for understanding customer service problems.

Example performance measures:

- Number of complaints per 1,000 customers (or other appropriate value based on size of population served) per reporting period, recorded as either customer service or technical quality complaints.
    - Customer service complaint rate: 1,000 X (customer service associated complaints ÷ number of active customer accounts). *This is a Benchmarking Performance Indicator*.
    - Technical quality complaint rate: 1,000 X (technical quality associated complaints ÷ number of active customer accounts). *This is a Benchmarking Performance Indicator*.

For both calculations, utilities may wish to subcategorize complaints by type and aspect (e.g., customer service into billing, problem responsiveness, interruptions, etc., and technical quality into service deficiencies such as taste, odor, appearance, flow/pressure, etc.) and by type of customer (e.g., residential, industrial, commercial, etc.)

2. Customer service delivery

Description: This measure requires the utility, based on internal objectives and customer input, to set desirable customer service levels, then determine an appropriate (target) percentage of time to meet the performance levels. Once established, the utility can track how often it meets the service levels, helping the utility to determine how well customer needs are being satisfied (e.g., have 95 percent of service calls received a response within 60 minutes). A utility can average across individual measures to determine the overall percentage of service level commitments met.

Example performance measures:

- Call responsiveness (percent): 100 X (number of calls responded to within "X" minutes ÷ total number of calls during reporting period) (typically per month).
- Error-driven billing adjustment rate (percent): 100 X (number of error-driven billing adjustments during reporting period ÷ number of bills generated during reporting period). *This is a Benchmarking Performance Indicator*.
- Service start/stop responsiveness (percent): 100 X (number of stop/start service orders processed within "X" days ÷ total number of stop/start service orders during reporting period).

---

[1] From AWWA and AwwaRF, *Selection and Definition of Performance Indicators for Water and Wastewater Utilities*, p. 41. 2004. Note: This material is copyrighted and any reprinting must be by permission of the American Water Works Association.

- First call resolution (percent): 100 X (number of calls for which problem was resolved/fixed/scheduled to be fixed at the time of the first call ÷ total number of calls during reporting period).

3. Customer satisfaction

Description: This is an overarching customer satisfaction measure based on requested customer feedback (surveys), not calls received or internal customer satisfaction service level commitments. A utility can measure customer satisfaction immediately after service provision or use a periodically performed, more comprehensive customer satisfaction survey. After-service surveys are simpler and easier for the utility to develop and implement without professional advice, but they tend to over represent the most satisfied (e.g., those who just received service) and the most dissatisfied (e.g., those who just called with complaints) customers. Comprehensive surveys can provide statistical validity enabling extrapolation to the population served. A utility can verify survey information through customer conversations, either as follow up to a survey, during public meetings or focus groups, or by some other method (e.g., individual telephone calls).

Example performance measures:

- Overall customer satisfaction: Percent of positive or negative customer satisfaction survey responses based on a statistically valid survey or on an immediately after-service survey. Satisfaction responses can be divided into categories such as: highly satisfied/satisfied/moderately satisfied/unsatisfactory; exceeding expectations/meeting expectations/not meeting expectations; numerical scales (e.g., 1-5); or other divisions. Customer satisfaction information is often also gathered and assessed by topic areas such as product quality, service reliability, billing accuracy, customer service, costs/rates/value, crew courtesy, notification around street construction/service interruptions, etc.

Employee and Leadership Development

1. Employee retention and satisfaction

Description: This measure gauges a utility's progress toward developing and maintaining a competent and stable workforce, including utility leadership.

Example performance measures:

- Employee turnover rate (percent): 100 X (number of employee departures ÷ total number of authorized positions per year). Can be divided into categories such as:
  - Voluntary turnover (percent): 100 X (number of voluntary departures ÷ total number of authorized positions per year). (Perhaps the best indicator of retention problems.)
  - Retirement turnover (percent): 100 X (number of retirement departures ÷ authorized positions per year). (Measures vulnerability to loss/retention of institutional knowledge.)
  - Experience turnover (percent): 100 X (number of years of experience represented by all departures ÷ total years of experience with the organization) (at the beginning of the year). (These are harder data to collect but provide a good assessment of institutional knowledge loss potential and therefore the need to retain/capture institutional knowledge.)

- Employee job satisfaction (percent): 100 X (number of employees with "X" job satisfaction level ÷ total number of employees) (based on implementation and monitoring over time of a comprehensive employee survey). Can be divided into work type or job classification categories, etc., and cover overall satisfaction and topics deemed relevant to longer-term employee satisfaction and retention, such as:
  - Compensation and benefits
  - Management
  - Professional development and long-term advancement opportunities
  - Work and teamwork
  - Procedures
  - Fairness and respect
  - Communication
  - Positive work environment
  - Recognition for achievements
- Employee salary competitiveness relative to market rate: Average percentile rank of employee salaries compared to salaries in surrounding service areas, as determined by a market rate comparison.

2. Management of core competencies

Description: This measure assesses the utility's investment in and progress toward strengthening and maintaining employee core competencies.

Example performance measures:

- Presence of job descriptions and performance expectations: Percentage of classifications with current job descriptions and related performance expectations.
- Training hours per employee: Total of qualified formal training hours for all employees ÷ total FTEs (FTE = 2,080 hours per year of employee time equivalent) worked by employees during the reporting period. *This is a Benchmarking Performance Indicator*.
- Certification coverage (percent): 100 X (number of certifications achieved or maintained ÷ number of needed certifications per year) (across the utility).
- Employee evaluation results (assumes utility evaluates employee performance in a routine way and documents results): Results of employee evaluations (e.g., employee growth not clearly demonstrated, employee growth only demonstrated in certain areas or for certain labor categories, etc.).
- Presence of employee-focused objectives and targets: Percentage of employees with written employee-focused organizational objectives and targets.(Targets could be, for instance, related to quantity, quality, timeliness, or cost. A timeliness target could, for example, relate to the number of hours it takes on average to complete a routine task.)

3. Workforce development

Description: This measure assesses utility long-term workforce succession planning efforts to ensure critical skills and knowledge are retained and enhanced over time, particularly in light of anticipated retirement

volume in coming years. Focus is on preparing entire groups or cohorts for needed workforce succession, including continued training and leadership development.

Example performance measures:

- Key position vacancies: Average time that critical-skill positions are vacant due to staff departures per vacancy per year.
- Key position internal/external recruitment (percent): 100 X (number of critical-skill positions that are filled internally (through promotion, transfer, etc. rather than outside recruitment) versus filled through outside recruitment ÷ total number of positions filled per year). (This will help the utility to understand if internal workforce development is covering long-term succession needs.)
- Long-term succession plan coverage (percent): 100 X (number of employees (or cohorts, work units, etc.) covered by a long-term workforce succession plan that accounts for projected retirements and other vacancies in each skill and management area ÷ total number of employees) (or cohorts, work units, etc.).
- Internal leadership development:
    - Percentage of staff and leadership positions with defined competencies.
    - Are internal or external leadership development/training/skills development opportunities provided to employees (yes/no)?

Operational Optimization

1. Resource optimization

Description: This measure examines resource use efficiency, including labor and material per unit of output or mile of collection/distribution system.

Example performance measures:

- Customer accounts per employee: Number of accounts ÷ number of FTEs. (FTE = 2,080 hours per year of employee time equivalent.) *This is a Benchmarking Performance Indicator*.
- MGD water delivered/processed per employee: Average MGD delivered/processed ÷ FTEs per year. *This is a Benchmarking Performance Indicator*.
- Chemical use per volume delivered/processed: Amount of chemicals used ÷ MG delivered/processed during reporting period. (Alternatively can use dollar amount spent on chemicals ÷ MG delivered/processed; in this case a rolling average for amount spent would account for periodic bulk purchases.)
- Energy use per volume delivered/processed: KWH ÷ MG delivered/processed during reporting period. (Alternatively can use dollar amount spent on energy ÷ MG delivered/processed.)
- O&M cost per volume delivered/processed: Total O&M cost ÷ MG delivered/processed during reporting period.

A utility can also apply the above resource use per volume delivered/processed calculations to resource use per mile (or 100 miles) of collection/distribution system, (i.e., chemical use per mile, energy use per mile, or O&M cost per mile).

2. Water management efficiency

Description: This measure assesses drinking water production and delivery efficiency by considering resources as they enter and exit the utility system.

Example performance measures:

- Production efficiency: Ratio of raw water volume taken into the treatment system to treated water produced.
- Meter function (percent): 100 X (total number of active billable meters minus stopped or malfunctioning meters ÷ total number of active billable meters).

Financial Viability

1. Budget management effectiveness

Description: This measure has short-term and long-term aspects. The short-term calculations are commonly used financial performance indicators, and the long-term calculation is a more comprehensive analytical approach to assessing budget health over the course of several decades.

Example performance measures:

Short-term (typically per year):

- Revenue to expenditure ratio: Total revenue ÷ total expenditures.
- O&M expenditures (percent): 100 X (O&M expenditures ÷ total operating budget).
- Capital expenditures (percent): 100 X (capital expenditures ÷ total capital budget).
- Debt ratio: Total liabilities ÷ total assets. Total liabilities are the entire obligations of the utility under law or equity. Total assets are the entire resources of the utility, both tangible and intangible. Utilities often have different debt-risk acceptability levels, thus the ratio itself should be considered within each utility's unique circumstances. *This is a Benchmarking Performance Indicator*.
- Current level of operating reserves as a percentage of goal.

Long-term:

- Life-cycle cost accounting: Has the utility conducted a life-cycle cost accounting analysis[2] that explicitly incorporates accepted service level risks, asset condition, budget needs based on the values (net present values) of utility current and future assets, etc., and made financial and budget management decisions accordingly (yes/no)?

---

[2] Section 707 of Executive Order 13123 defines life-cycle costs as, "…the sum of present values of investment costs, capital costs, installation costs, energy costs, operating costs, maintenance costs, and disposal costs over the life-time of the project, product, or measure." Life-cycle cost analysis (LCCA) is an economic method of project evaluation in which all costs arising from owning, operating, maintaining, and disposing of a [facility/asset] are considered important to the decision. LCCA is particularly suited to the evaluation of design alternatives that satisfy a required performance level, but that may have differing investment, operating, maintenance, or repair costs; and possibly different life spans. LCCA can be applied to any capital investment decision, and is particularly relevant when high initial costs are traded for reduced future cost obligations. See also: https://energy.gov/nepa/downloads/eo-13148-greening-government-through-leadership-environmental-management-2000, http://www.wbdg.org/resources/lcca.php.

2. Financial procedure integrity

Description: This measure gauges the presence of internal utility processes to ensure a high level of financial management integrity.

Example performance measures:

- Number of control deficiencies and material weaknesses reported on annual audits.
- Does the utility have financial accounting policies and procedures (yes/no)?
- Are financial results and internal controls audited annually (yes/no)?
- Have the number of control deficiencies and material weaknesses been reduced from previous audits (yes/no)?
- Does the utility have a formal policy for the bill collection process (yes/no)?

3. Bond ratings

Description: This measure uses bond ratings as a general indicator of financial viability; however, they are not always within a utility's control and are less important if a utility is not participating in capital markets. Smaller utilities often struggle to obtain high ratings. Even though a higher bond rating is desirable and this provides a general indicator of financial health, the bond rating should not be considered alone. It should be considered in light of other factors such as the other measures suggested for this Attribute.

Example performance measure:

- Bond ratings.
- Change in bond ratings: Does the change reflect the utility's financial management in a way that can and should be acknowledged and, if need be, addressed?

4. Rate adequacy

Description: This measure helps the utility to consider its rates relative to factors such as external economic trends, short-term financial management, and long-term financial health. It recognizes that a "one size fits all" calculation would not be realistic due to each utility's unique situation and the number of variables that could reasonably be considered. The following three questions prompt assessment of key components of rate adequacy.

Example performance measures:

- How do your rate changes compare currently and over time with the inflation rate and the Consumer Price Index (CPI) or Consumer Price Index for All Urban Consumers (CPI-U)? (Rate increases below CPI for very long may suggest rates are not keeping up with utility costs.) (Using a rolling rate average over time will adjust for short-term rate hikes due to capital or O&M spending needs.)
- Have you established rates that fully consider the full life-cycle cost of service and capital funding options? (See the life-cycle cost accounting discussion, above.)
- Does your utility maintain a rate stabilization reserve to sustain operations during cycles of revenue fluctuation, in addition to 60- (or 90-) day operating reserves?

Infrastructure Strategy and Performance

1. Asset inventory

Description: This measure gauges a utility's efforts to assess assets and asset conditions, as the first steps towards building a comprehensive asset management program.

Example performance measures:

- Inventory coverage (percent): 100 X (total number of critical assets inventoried within a reasonable period of time (e.g., 5-10 years) ÷ total number of critical assets). A utility will need to first define what it considers to be a critical asset. Typically, critical assets are those that you decide would have major consequences if they were to fail (major expense, system failure, safety concerns, etc.). A complete inventory will involve understanding the following for each asset:
    - Age and location;
    - Asset size and/or capacity;
    - Valuation data (e.g., original and replacement cost);
    - Installation date and expected service life;
    - Maintenance and performance history; and
    - Construction materials and recommended maintenance practices.[3]
- Condition assessment coverage (percent): 100 X (total number of critical assets with condition assessed and categorized into condition categories within a reasonable period of time (e.g., 5-10 years) ÷ total number of critical assets). Condition categories could include: unacceptable, improvement needed, adequate, good, and excellent to reflect expected service levels and acceptable risks.

2. Asset (system) renewal/replacement

Description: This measure assesses asset renewal/replacement rates over time. The measure should reflect utility targets, which will vary depending on each utility's determinations of acceptable risks for different asset classes. An asset class may consist of a cohort of pipe based on age/material, or a particular component of plants or lift stations. Generally, an asset class would have an expected service life, and this should be factored into calculations for an appropriate asset renewal/replacement rate. Decisions on asset replacement typically factor in internally agreed-upon risks and objectives, which may differ by asset class and other considerations. For instance, a utility may decide to run certain assets to failure based on benefit-cost analysis.

Example performance measures:

- Asset renewal/replacement rate (percent): 100 X (total number of assets replaced per year for each asset class ÷ total number of assets in each asset class). For example, a two percent per year replacement target (50-year renewal) for a particular asset class could be identified as the basis for performance monitoring.

    — or —

---

[3] From the U.S. General Accounting Office, *Water Infrastructure: Comprehensive Asset Management Has Potential to Help Utilities Better Identify Needs and Plan Future Investments*. GAO-04-461. March 2004. Available: http://www.gao.gov/new.items/d04461.pdf.

- Asset (system) renewal/replacement rate: 100 X (total actual expenditures or total amount of funds reserved for renewal and replacement for each asset group ÷ total present worth for renewal and replacement needs for each asset group). *This is a Benchmarking Performance Indicator*.

3. Water distribution/collection system integrity

Description: For drinking water utilities, this measure quantifies the number of pipeline leaks and breaks. Distribution system integrity has importance for health, customer service, operational, and asset management reasons. For wastewater utilities, this measure examines the frequency of collection system failures. When tracked over time, a utility can evaluate whether its failure rate is decreasing, stable, or increasing. When data are maintained to characterize failures by pipe type and age, type of failure, and cost of repairs, decisions regarding routine maintenance and replacement/renewals can be better made.

Example performance measure (drinking water utilities):[4]

- Non-revenue water (NRW): Water supplied to the network that does not return revenue to the utility, including unbilled authorized consumption, apparent losses (theft, customer metering inaccuracies, systematic data handling errors), and real losses (leakage from the pipe network and distribution storage) as defined in the AWWA M36 Manual. May be expressed as volume or value:
  - Volume:
    - Total volume for audit year; and/or
    - Volume per connection per year; and/or
    - Volume per connection per day.
  - Value:
    - Total cost of NRW by total cost of water system operations; and/or
    - Cost of NRW per connection per year.
- Infrastructure leakage index (ILI): Current Annual Real Loss ÷ Unavoidable Annual Real Loss (at current average system operating pressure. Measure would be expressed as a unitless ratio. *Automatic derivation of this measure provided in the AWWA Free Water Audit Software from annual water audit inputs.*
- Audit Validation Level: Level of validation (self-reported, 1, 2 or 3) conducted on the most recent water audit, as defined by Water Research Foundation Project 4639A.[5]

Example performance measure (wastewater utilities):

- Collection system failure rate (percent): 100 X (total number of collection system failures ÷ total miles of collection system piping per year). *This is a Benchmarking Performance Indicator*.

4. Infrastructure planning and maintenance

Description: This measure addresses planning for future infrastructure needs and ongoing maintenance for existing infrastructure, which is critical to overall infrastructure strategy and performance. Planned maintenance includes both preventive and predictive maintenance. Preventive maintenance is performed

---

[4] For more information, visit: http://www.awwa.org/store/productdetail.aspx?productid=51439782 and http://www.awwa.org/resources-tools/water-knowledge/water-loss-control.aspx.
[5] For more information, visit: *http://www.waterrf.org/Pages/Projects.aspx?PID=4639*

according to a predetermined schedule rather than in response to failure. Predictive maintenance is initiated when signals indicate that maintenance is due. All other maintenance is categorized as corrective or reactive.

Example performance measures:

This measure can be approached in different ways. Calculating costs may be preferable to encourage business decisions based on total cost; however, the reliability of costs is uncertain. Hours are likely to be less variable than costs, but not all utilities track hours. Thus, cost and hours ratios are desirable, where possible.

- Planned maintenance ratio by hours (percent): 100 X (hours of planned maintenance ÷ (hours of planned + corrective maintenance)). *This is a Benchmarking Performance Indicator*.
- Planned maintenance ratio by cost (percent): 100 X (cost of planned maintenance ÷ (cost of planned + corrective maintenance)). *This is a Benchmarking Performance Indicator*.
- Is there a formal process to prioritize infrastructure needs/future investments and allocate the necessary funding (yes/no)?
- Is there a formal process for identifying areas of uncertainty and building in needed flexibility during the infrastructure planning phase (yes/no)?

Enterprise Resiliency

1. Recordable incidents of injury or illnesses

Description: This measure addresses incidence rates, which can be used to show the relative level of injuries and illnesses and help determine problem areas and progress in preventing work-related injuries and illnesses.

Example performance measure:

The U.S. Bureau of Labor Statistics has developed instructions for employers to evaluate their firm's injury and illness record. The calculation below is based on these instructions, which can be accessed at: http://www.bls.gov/iif/osheval.htm. The 200,000 hours used in the formulas below represent the equivalent of 100 employees working 40 hours per week, 50 weeks per year, and provides the Bureau of Labor Statistics' standard base for the incidence rates.

- Total recordable incident rate: (Number of work-related injuries and illnesses X 200,000) ÷ employee hours worked.
- Number of near misses: A "near miss" is an unsafe situation or condition where no personal injury was sustained and no property was damaged, but where, given a slight shift in time or position, injury and/or damage could have occurred.

2. Insurance claims

Description: This measure examines the number, type, and severity of insurance claims to understand insurance coverage strength/vulnerability.

Example performance measures:

- Number of insurance claims: Number of general liability and auto insurance claims per 200,000 employee hours worked.

- Severity of insurance claims: Total dollar amount of general liability and auto insurance claims per 200,000 employee hours worked.

3. Risk assessment and response preparedness

Description: This measure asks whether utilities have assessed their all-hazards (natural and human-caused) vulnerabilities and risks and made corresponding plans for critical needs. Risk assessment in this context includes a vulnerability assessment regarding, for example, power outages, lack of access to chemicals, cybersecurity, extreme weather events, curtailed staff availability, etc.

Example performance measures:

- Emergency Response Plan (ERP) coverage and preparedness:
  - Does the utility have an ERP in place (yes/no)?
  - Number and frequency of ERP exercises per year: 100 X (number of critical employees who participate in ERP exercises ÷ total number of critical employees).
  - Frequency with which the ERP is reviewed and updated.
  - Does the utility discuss/coordinate ERP with other agencies/departments (e.g., city, state, police, fire, public health) (yes/no)?
- Vulnerability management: Is there a process in place for identifying and addressing system deficiencies (e.g., deficiency reporting with an immediate remedy process, established intervals between comprehensive vulnerability assessments) (yes/no)?

4. Ongoing operational resiliency

Description: This measure assesses a utility's operational reliability during ongoing/routine operations.

Example performance measure:

- Uptime for critical utility components on an ongoing basis (percent): 100 X (hours of critical component uptime ÷ hours that critical components have the physical potential to be operational). Note: a utility can apply this measure on an individual component basis or summed across all identified critical components. Also, a utility can make this measure more precise by adjusting for planned maintenance periods.
- Cybersecurity:
  - Does the utility document and periodically review network architecture (including defining network boundaries and network asset inventory)? (yes/no) *This is a Benchmarking Performance Indicator.*
  - Does the utility implement formal, written cybersecurity policies that include specific operational aspects associated with service delivery and assurance (not enterprise)? (yes/no) *This is a Benchmarking Performance Indicator.*

5. Operational resiliency under emergency conditions

Description: This measure assesses the operational preparedness and expected responsiveness in critical areas under emergency conditions.

Example performance measures (all apply to emergency conditions and, where relevant, factor in anticipated downtimes relative to required/high demand times):

- Power resiliency: Period of time (e.g., hours or days) for which backup power is available for critical operations (i.e., those required to meet 100 percent of minimum daily demand). (Note: "minimum daily demand" is the average daily demand for the lowest production month of the year.)
- Treatment chemical resiliency: Period of time (e.g., hours or days) minimum daily demand can be met with water treated to meet SDWA standards for acute contaminants (i.e., E.coli, fecal coliform, nitrate, nitrite, total nitrate and nitrite, chlorine dioxide, turbidity as referenced in the list of situations requiring a Tier 1 Public Notification under 40 CFR 141.202), without additional treatment chemical deliveries. (Note: "minimum daily demand" is the average daily demand for the lowest production month of the year.)
- Critical parts and equipment resiliency: Current longest lead time (e.g., hours or days) for repair or replacement of operationally critical parts or equipment (calculated by examining repair and replacement lead times for all identified critical parts and equipment and taking the longest single identified time).
- Critical staff resiliency: Average number of response-capable backup staff for critical operation and maintenance positions (calculated as the sum of all response-capable backup staff ÷ total number of critical operation and maintenance positions).
- Treatment operations resiliency (percent): Percent of minimum daily demand met with the primary production or treatment plant offline for 24, 48, and 72 hours. (Note: "minimum daily demand" is the average daily demand for the lowest production month of the year.)
- Sourcewater resiliency: Period of time (e.g., hours or days) minimum daily demand can be met with the primary raw water source unavailable. (Note: "minimum daily demand" is the average daily demand for the lowest production month of the year.)

Community Sustainability

1. Watershed-based infrastructure planning

Description: This measure addresses utility efforts to consider watershed-based approaches when making management decisions affecting infrastructure planning and investment options. Watershed protection strategies can sometimes, for example, protect source water quality limiting the need for additional or enhanced water treatment capacity.

Example performance measure:

- Does the utility employ alternative, watershed-based approaches to align infrastructure decisions with overall watershed goals and potentially reduce future infrastructure costs (yes/no)? Watershed-based approaches include, for example: centralized management of decentralized systems; stormwater management; source water protection programs; and conjunctive use of groundwater, source water, and recycled water to optimize resource use at a basin scale. (See also "green infrastructure" below.)

2. Green infrastructure

Description: This measure addresses green infrastructure, which includes both the built and natural/unbuilt environment. Utilities may promote source water protection and conservation green infrastructure approaches in support of water conservation (e.g., per capita demand reduction) and water quality protection objectives. Green infrastructure approaches can include: low-impact development techniques (e.g., minimization of impervious surfaces, green roofs); protection of green spaces and wildlife habitat; incentives for water-efficient domestic appliance use and landscaping; green building standards such as those promoted through the Leadership in Energy and Environmental Design (LEED) program; management of energy, chemical, and material use; etc.[6] Utilities often coordinate these efforts with community planning offices.

Example performance measures:

- Has the utility explored green infrastructure approaches and opportunities that are aligned with the utility's mandate, goals, and objectives and community interests (yes/no)?
- Does the utility have procedures that incorporate green infrastructure approaches and performance into new infrastructure investments (yes/no)?

3. Greenhouse gas emissions

Description: This measure will help drinking and wastewater utilities to understand and reduce their individual contributions to area greenhouse gas emissions. Trends indicate that water utility emissions of these gases will likely be of interest to stakeholders. Monitoring of these emissions is becoming more common among water sector utilities, and some utilities are beginning voluntary efforts to reduce their emissions (e.g., through production of reusable methane energy by wastewater utilities).

Example performance measures:

- Net (gross minus offsets) greenhouse gas emissions in tons of carbon dioxide (CO_2), nitrous oxide (N_2O), methane (CH_4), and, as applicable, hydrofluorocarbons (HFCs) and perfluorocarbons (PFCs). Start by establishing an emissions baseline and then track emission trends in conjunction with minimizing/reducing emissions over time, where possible.[7] Emissions inventories often incorporate indirect emissions such as those generated during the production and transport of materials and chemicals.
- Percent of utility energy demand met by renewable energy resources.

4. Service affordability

Description: This measure addresses drinking water and wastewater service affordability, which centers on community members' ability to pay for water services. The true cost of water/wastewater services may be higher than some low-income households can afford, particularly when rates reflect the full life-cycle cost of water services. To the extent possible within its operating and regulatory contexts, the utility will want to

---

[6] For more information about green infrastructure, visit https://www.epa.gov/npdes/green-infrastructure.

[7] EPA's industry-government "Climate Leaders" partnership involves completing a corporate-wide inventory of their greenhouse gas emissions. Information and related guidance is available at http://www.epa.gov/stateply/index.html.

consider and balance keeping water services affordable while ensuring the rates needed for long-term infrastructure and financial integrity.

Example performance measures:

- Bill affordability (households for which rates may represent an unaffordable level) (percent): 100 X (number of households served for which average water bill is > "X" percent (often 2-2.5%) of median household income[8] ÷ total number of households served).

Coupled with:

- Low-income billing assistance program coverage (percent): 100 X (number of customers enrolled in low-income billing assistance program ÷ number of customers who are eligible for enrollment in low-income billing assistance program). (The utility can try to increase participation in the program for eligible households that are not participating).

5. Community economic development

Description: This measure assesses the extent to which utility operations play a role in local economic development (e.g., by attracting new employers to the area, enabling residential or commercial growth, or through job creation).

Example performance measures:

- Change in tax base (dollars or percent change) related to new water infrastructure.
- Number of jobs created by utility infrastructure investments. Jobs may be:
    - Internal to the utility;
    - Contracted by the utility; or
    - Through a new employer brought to the community as a result of utility infrastructure.
- Green infrastructure economic benefits:
    - Crime reduction (percent change); and
    - Increase in local property values (percent change).

Water Resource Sustainability

1. Water supply adequacy

Description: This measure assesses short-term and long-term water supply adequacy and explores related long-term supply considerations.

Example performance measures:

- Short-term water supply adequacy: Period of time for which existing supply sources are adequate. This can be measured as a ratio of projected short-term (e.g., 12-month rolling average) monthly

---

[8] This calculation focuses on identifying low-income households based median household incomes (MHI); however, MHI is not strongly correlated with the incidence of poverty or other measures of economic need. Further, populations served by small utilities in rural settings tend to have lower MHI and higher poverty rates, but fewer options for diversifying water/wastewater service rates based on need compared to larger municipal systems.

supply to projected short-term monthly demand. Often an index or scale is used, for example, short-term supply relative to severe drought (assigned a "1") to abundant supply conditions (assigned a "5").

- Long-term water supply adequacy: Projected future annual supply relative to projected future annual demand for at least the next 50 years (some utilities project out as far as 70-80 years). Statistical forecasting and simulation modeling and forecasting techniques are typically used for such long-term projections. Analysis variables in addition to historical record (e.g., historical and year-to-date reservoir elevation data), forecasted precipitation, and flows (including surface and groundwater, as applicable) can include:
    - Future normal, wet, dry, and very dry scenarios;
    - Anticipated population changes;
    - Future service areas;
    - Availability of new water supplies including both traditional, and alternative supplies, such as recycled water, groundwater banking, desalinization, or groundwater highest and best use; and
    - Levels of uncertainty around the above.
- Water Reuse (water beneficially reused):
    - Amount (percentage or gallons) of reclaimed water used in place of fresh water or drinking water for non-potable uses.
    - Amount (percentage or gallons) of reclaimed water used for potable purposes.
    - Amount (gallons or acre feet) of reclaimed water added to drinking water reservoir(s).
    - Area (acres) of land irrigated using only recycled water.

2. Supply and demand management

Description: This measure explores whether the utility has a strategy for proactive supply and demand management in the short and long terms. Strategy needs will depend on community circumstances and priorities, anticipated population growth, future water supply in relation to anticipated demand, demand management and other conservation options, and other local considerations.

Example performance measures:

- Does the utility have a demand management/demand reduction plan (yes/no)? Does this plan track per capita water consumption and, where analytical tools are available to do so, accurately attribute per capita consumption reductions to demand reduction strategies (such as public education and rebates for water-efficient appliances) (yes/no)?
- Do demand scenarios account for changes in rates (which can change for many reasons) and conservation-oriented, demand management pricing structures (yes/no)?
- Does the utility have policies in place that address, prior to committing to new service areas, the availability of adequate dry year supply (yes/no)? Alternatively, does the utility have a commitment to denying service commitments unless a reliable drought-year supply, with reasonable drought use restrictions, is available to meet the commitment (yes/no)?

3. Watershed sustainability

Description: This measure explores whether the utility has a strategy for proactive watershed management and/or partnerships to ensure an effective integration of utility and watershed investments and practices, to achieve overall optimized performance for the community and the utility.

Example performance measures:

- Amount of pollutants/contaminants managed through source control practices (avoiding the need for treatment plant upgrades, etc.).
- Has the utility developed a source water protection plan (yes/no)?
- Does the utility partner with regional stakeholders to protect and enhance its watershed (yes/no)?
- Percent of wet weather impacts (e.g., flooding, CSOs, SSOs, gallons of infiltrated water not reaching collection systems) managed through watershed (natural treatment) processes: 100 X (Number of wet weather impacts managed through watershed processes ÷ total number of wet weather impacts).
- Area (in acres) of enhancements to wetland areas for treatment/storage of wet weather flows.
- Amount of nutrient removal via watershed approaches:
  - Cost savings derived from nutrient control through watershed processes as an alternative to treatment plant nutrient removal; and
  - Percent of nutrient removal requirements met through watershed processes rather than treatment at the plant.
- Environmental benefits:
  - Amount of movement or reduction of saltwater front (in feet).
  - Amount of avoided freshwater diversion from sensitive ecosystems.

Stakeholder Understanding and Support

1. Stakeholder consultation

Description: This measure addresses utility actions to reach out to and consult with stakeholders about utility matters, including utility goals, objectives, and management decisions.

Example performance measures:

- Does the utility identify stakeholders, conduct outreach, and actively consult with stakeholders about utility matters (yes/no)? Elements of this plan can include:
  - Number of active contacts with stakeholders in key areas (e.g., from local government, business, education, non-governmental groups)?
  - Does the utility actively seek input from stakeholders (yes/no)?
  - Frequency with which the utility actively consults with stakeholders. This measure should go beyond counting the number of calls or times information is sent out or posted on websites to items such as number of stakeholder outreach and education activities, number of opportunities for stakeholders to provide input, participation of stakeholders on utility committees, etc.
- Does the utility actively consider and act upon stakeholder input (yes/no)?

2. Stakeholder satisfaction

Description: This measure addresses stakeholder perceptions of the utility. Stakeholder satisfaction can be measured through surveys sent to stakeholders, formal feedback surveys distributed to stakeholders at events, etc.

Example performance measures:

- Overall satisfaction (percent): 100 X (number of stakeholders who annually rate the overall job of the utility as positive ÷ total number of stakeholders surveyed).
- Responsiveness (percent): 100 X (number of stakeholders who annually rate utility responsiveness to stakeholder needs as positive ÷ total number of stakeholders surveyed).
- Message recollection for outreach programs targeted to specific stakeholder groups (percent): (a) 100 X (number of stakeholders who recall key messages ÷ total number of stakeholders surveyed); and (b) 100 X (number of stakeholders who recall the message source (TV, utility mailers, newsletters, etc.) ÷ total number of stakeholders surveyed).

3. Internal benefits from stakeholder input

Description: This measure addresses the value utility employees believe stakeholder engagement has provided to utility projects and activities. Measurement by the utility can focus on surveying utility employees running projects that have stakeholder involvement.

Example performance measures:

- 100 X (number of utility projects or activities where stakeholders participated and/or provided input for which utility employees believe there was value added as a result of stakeholder participation and input ÷ total number of projects where stakeholders participated and/or provided input).
- Overall value added (percent): 100 X (number of utility employees who rated their overall sense of value added from stakeholder participation and input as (high value added, some value added, little value added, no value added) ÷ total number of utility employees surveyed).

4. Comparative rate rank

Description: This measure depicts how utility rates compare to similar utilities (e.g., utilities of the same type (drinking water, wastewater) that are similar in terms of geographic region, size of population served, etc.). A utility can use the measure internally or to educate stakeholders. It should be noted that the lowest rate is not necessarily best (see Financial Viability). When comparing rates with other utilities, it is important to make sure to account for other variables that can affect rates to ensure that you are comparing "apples to apples." For example, when comparing a wastewater collection and treatment utility's rates to a utility providing treatment only, include the average rate of the separate wastewater collection utility in a combined rate.

Example performance measure:

- Typical monthly bill for the average household as a percentage of typical monthly bills for similar utilities.

5. Media/press coverage

Description: This measure captures media portrayal of the utility (newspaper, TV, radio, etc.) in terms of awareness, accuracy, and tone.

Example performance measures:

- Amount of coverage: Total number of media stories (social media, newspaper, TV, radio, etc.) concerning the utility per year.
- Media coverage tone (percent): 100 X (number of media stories concerning the utility that portray the utility in a positive way ÷ total number of media stories concerning the utility) per year.
- Media coverage accuracy (percent): 100 X (number of media stories that accurately describe the utility ÷ total number of media stories concerning the utility) per year.
- Number of outreach events conducted to build support for utility, value of water, and value of water services.

6. Partnering in your community

Description: This measure assesses how the utility actively engages with community organizations to advance important initiatives, engage partners in decision making, and to position the utility as an anchor institution in the community. Partnering in this manner can result in many different types of benefits for the utility and the community, including the increased understanding and support for utility needs and the value of water and water services to the community.

Example performance measures:

- Performance improvements resulting from a partnership (e.g., reduced volume of flooding or greenhouse gas emissions).
- Number and type of specific projects completed associated with partnerships (e.g., rain gardens installed, innovative technologies implemented, innovative practices adopted).
- Level of partner/community support for utility and the value of water (e.g., number of community members/partners participating in utility events or providing positive feedback for utility services).

ADDITIONAL ATTRIBUTE-SPECIFIC MEASUREMENT RESOURCES

The following resources provide additional measures that are specific to various Attributes. The list is not meant to be exhaustive, but rather, serves as a starting place for utilities seeking additional resources for measures.

- **The Energy Roadmap** (Water Environment Federation)
- **National Biosolids Partnership** (Water Environment Federation)
- **The Nutrient Roadmap** (Water Environment Federation)
- **On-Demand WasteWater Library (OWWL)** (Water Environment Federation)
- **The Value of Water** (http://thevalueofwater.org/)
- **Work for Water** (American Water Works Association and Water Environmental Federation)
- **Water Advocates** (Water Environment Federation)
- **AWWA Water and Wastewater Rate Survey** (American Water Works Association) *subscriber only*
- **AWWA Compensation Survey** (American Water Works Association) *subscriber only*
- **NACWA Financial Survey** (National Association of Clean Water Agencies)

Effective Utility Management: A Primer for Water and Wastewater Utilities

January 2017

Appendix J

AWWA CYBERSECURITY RESULTS MANATEE

Category	Control	Priority	Referenced Standards	Level Of Implementation	Project	Notes
AT-3	A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.	Priority 1 Controls	DHS CAT: 2.7.7 Investigation and Analysis	Not Implemented		
IA-1	Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.	Priority 1 Controls	AWWA G430-14: 4.6 Access Control and Intrusion Detection / NIST 800-82r2: 6.2.1 Access Control	Not Implemented		
IA-10	Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.	Priority 1 Controls	DHS CAT: 2.15.11 Permitted Actions without ID or Authentication	Not Implemented		
IA-12	Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.	Priority 1 Controls	ISA 62443-3-3: 9.3 Network Segmentation NIST 800-53: Appendix F-SC: SC-7 Boundary Protection NIST 800-82r2: 5.6 Recommended Defense-in-Depth Architecture	Not Implemented		
IA-3	Role based access control system established including policies and procedures.	Priority 1 Controls	DHS CAT: 2.15 Access Control / NIST 800-53: Appendix F-AC: AC-3 Access Enforcement	Not Implemented		
IA-4	Access control for confidential system documentation established to prevent unauthorized access of trade secrets, program source code, documentation, and passwords (including approved policies and procedures).	Priority 1 Controls	DHS CAT: 2.5.5 Control System Documentation NIST 800-53: Appendix F-AC: AC-3 Access Enforcement ISO/IEC 27001: Annex A: A.13.1.1 Network Controls	Not Implemented		
IA-5	Access control for diagnostic tools and resources and configuration ports.	Priority 1 Controls	NIST 800-53: Appendix F-AC: AC-3 Access Enforcement NIST 800-53: Appendix F-AC: AC-17 Remote Access	Not Implemented		
IA-6	Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.	Priority 1 Controls	NIST 800-82r2: 5.15 Authentication and Authorization	Not Implemented		
PE-1	Security perimeters, card controlled gates, manned booths, and procedures for entry control.	Priority 1 Controls	DHS CAT: 2.4.3 Physical Access Control, NIST 800-53: Appendix F-PE: PE-3 Physical Access Control, ISO/IEC 27001: Annex A: A.11.1.1 Physical security perimeter	Partially Implemented		
PE-2	Secure areas protected by entry controls and procedures to ensure that only authorized personnel have access.	Priority 1 Controls	ISO/IEC 27001: Annex A: A.11.1 Secure areas, NIST 800-53: Appendix F-PE: PE-5 Access Control for Output Devices	Partially Implemented		
PE-3	Physical security and procedures for offices, rooms, and facilities.	Priority 1 Controls	ISO/IEC 27001: Annex A: A.1.1.3 Securing offices and facilities, NIST 800-53: Appendix F-PE: PE-4 Access Control for Transmission Medium	Partially Implemented		
PE-4	Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.	Priority 1 Controls	DHS CAT: 2.4 Physical and Environmental Security, ISO/IEC 27001: Annex A: A.11.1.4 Protecting against external and environmental threats, NIST 800-53: Appendix F-CP: CP-2 Contingency Plan	Partially Implemented		
PE-5	Physical security and procedures for working in secure areas.	Priority 1 Controls	ISO/IEC 27001: Annex A: A.11.1.5 Working in secure areas, NIST 800-53: Appendix F-PE: PE-1 Physical and Environmental Policy and Procedures	Partially Implemented		
PE-6	Physical security and procedures for mail rooms, loading areas, etc., established. These areas must be isolated from IT/PCS areas	Priority 1 Controls	ISO/IEC 27001: Annex A: A.11.1.6 Delivery and Loading areas, NIST 800-53: Appendix F-PE: PE16 Delivery and Removal	Not Implemented		
PE-7	Physical security and procedures against equipment environmental threats and hazards or unauthorized access.	Priority 1 Controls	DHS CAT: 2.4 Physical and Environmental Security,ISO/IEC 27001: Annex A: A.11.1.4 Protecting against external and environmental, NIST 800-53: Appendix F-CP: CP-7 Alternate Processing Site	Partially Implemented		
PE-8	Physical/logical protection against power failure of equipment (UPS).	Priority 1 Controls	ISO/IEC 27001: Annex A: A.11.2.2 Supporting utilities, NIST 800-53: Appendix F-CP: CP-8 Telecommunications Services	Fully Implemented and Maintained		
PE-9	Physical/logical protection against access to power and telecommunications cabling established.	Priority 1 Controls	ISO/IEC 27001: Annex A: A.11.2.3 Cabling security, NIST 800-53: Appendix F-PE: PE-9 Power Equipment and Cabling	Partially Implemented		
SC-1	Policies and procedures governing cryptography and cryptographic protocols including key/certificate-management established to maximize protection of systems and information.	Priority 1 Controls	DHS CAT: 2.8.11 Cryptographic Key Establishment and Management, ISA 62443-3-3: 9 Restricted Data Flow, NIST 800-82r2: 6.2.16.1 Encryption	Not Implemented		
SC-12	Remote access framework including policies and procedures established to provide secure access to telecommuting staff, established for the management, monitoring, review, and audit of remote access to the organization.	Priority 1 Controls	NIST 800-53: Appendix F-AC: AC-17 Remote Access	Not Implemented		
SC-14	Network segregation. Firewalls, deep packet inspection and/or application proxy gateways.	Priority 1 Controls	NIST 800-82r2: 5.1 Network Segmentation and Segregation	Partially Implemented		
SC-15	Logically separated control network. Minimal or single access points between corporate and control network. Stateful firewall between corporate and control networks filtering on TCP and UDP ports. DMZ networks for data sharing.	Priority 1 Controls	NIST 800-82r2: 5.4 Logically Separated Control Network	Not Implemented		
SC-16	Defense-in-depth. Multiple layers of security with overlapping functionality.	Priority 1 Controls	NIST 800-82r2: 5.5 Network Segregation	Not Implemented		
SC-17	Virtual Local Area Network (VLAN) for logical network segregation.	Priority 1 Controls	NIST 800-82r2: 6.2.1.3 Virtual Local Area Network (VLAN)	Not Implemented		
SC-2	Centralized authentication system or single sign-on established to authorize access from a central system.	Priority 1 Controls	DHS CAT: 2.15.16 Passwords	Not Implemented		
SC-23	Wireless communications links encrypted.	Priority 1 Controls	NIST 800-82r2: 6.2.1.5 Wireless	Not Implemented		
SC-24	Communications links encrypted.	Priority 1 Controls	NIST 800-82r2: 6.2.1.5 Wireless	Not Implemented		
SC-25	Virtual Private Network (VPN) using IPsec, SSL or SSH to encrypt communications from untrusted networks to the control system network.	Priority 1 Controls	NIST 800-82r2: 5.10.2 Remote Support Access, NIST 800-82r2: 5.4 Logically Separated Control Network	Not Implemented		
SC-3	Policies and procedures established for network segmentation including implementation of DMZs based on type and sensitivity of equipment, user roles, and types of systems established.	Priority 1 Controls	ISA 62443-3-3: 9.2 Restricted Data Flow Rationale, NIST 800-82r2: 5.5.4 Firewall with DMZ between Corporate Network and Control Network	Not Implemented		
SI-1	Electronic commerce infrastructure in place providing integrity, confidentiality and non-repudiation and including adherence to pertinent laws, regulations, policies, procedures, and approval by management.	Priority 1 Controls	NIST 800-53: Appendix F-AU: AU-10 Non-Repudiation	Not Applicable		
SI-3	Interactive system for managing password implemented to ensure password strength.	Priority 1 Controls	NIST 800-53: Appendix F-IA: IA-5 Authenticator Management	Not Implemented		
AT-1	A security awareness and response program established to ensure staff is aware of security policies and incident response/notification procedures.	Priority 2 Controls	DHS CAT: 2.11 Security Awareness and Training, ISA 62443-2-1: A.3.2.4 Staff Training and Security Awareness	Not Implemented		

Control	Description	Priority	Standards	Status
AT-2	Security training including Incident response training for employees, contractors and third party users based on job roles.	Priority 2 Controls	AWWA G430-14: 4.3 Defined Security Roles and Employee Expectations DHS CAT: 2.11.3 Security Training	Not Implemented
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.	Priority 2 Controls	ISA 62443-3-3: 6 Use Control NIST 800-82r2: 6.2.3 Audit and Accountability	Not Implemented
AU-2	Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.	Priority 2 Controls	DHS CAT: 2.1 Security Policy, ISO/IEC 27001: Annex A: A.5 Information security policy	Not Implemented
AU-3:	Governance framework to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.	Priority 2 Controls	ISA 62443-2-1: A.3.2.3 Organizing for security, ISO/IEC 27005: 27005 Whole Document, NIST 800-53: Appendix J: AR-1 Governance and Privacy Program	Not Implemented
AU-4	Information security responsibilities defined and assigned.	Priority 2 Controls	ISO/IEC 27001: Annex A: A.6.1.1 Information systems roles and responsibilities NIST 800-53: Appendix F-AU: AU-1 Audit and Accountability Policies and Procedures	Not Implemented
AU-5	Risk based business continuity framework established under the auspices of the executive team to maintain continuity of operations and consistency of policies and plans throughout the organization. Another purpose of the framework is to ensure consistency across plans in terms of priorities, contact data, testing, and maintenance.	Priority 2 Controls	DHS CAT: 2.12.2 Continuity of Operations Plan ISA 62443-2-1: A.3.2.5 Business continuity plan ISO/IEC 27003: 27003 8.2 Conduct risk assessment	Not Implemented
AU-6	Policies and procedures established to validate, test, update and audit the business continuity plan throughout the organization.	Priority 2 Controls	NIST 800-124: 2.2.1-5 Lack of Physical Security Controls	Not Implemented
AU-7	Policies and procedures for system instantiation/deployment established to ensure business continuity.	Priority 2 Controls	ISO/IEC 27001: Annex A: A.14.2.9 System acceptance testing ISA 62443-2-1: A.3.3.5.3 Separation of duties	Not Implemented
CM-3	Separation of duties implemented for user processes including risk of abuse.	Priority 2 Controls	ISO/IEC 27001: Annex A: A.6.1.2 Segregation of duties NIST 800-53: Appendix F-AC: AC-5 Separation of Duties	Not Implemented
CM-5	SLAs for all third parties established, including levels of service and change controls.	Priority 2 Controls	DHS CAT: 2.5.9 Outsourced Control System Services NIST 800-53: Appendix F-SA: SA-9 External Information System Services	Not Implemented
CM-7	Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.	Priority 2 Controls	DHS DID: 3.4 Intrusion Detection Systems NIST 800-53: Appendix F-CM: CM-11 User-Installed Software	Not Implemented
IA-11	Workstation and other equipment authentication framework established to secure sensitive access from certain high risk locations.	Priority 2 Controls	DHS CAT: 2.15.5 Authenticator Management ISA 62443-1-1: 5.3 Defense in Depth	Not Implemented
IA-9	Multifactor authentication system established for critical areas.	Priority 2 Controls	ISA 62443-3-3: 5.3 Human User ID and Authentication NIST 800-34: 3.2 Conduct the Business Impact Analysis NIST 800-82r2: 6.2.7 Identification and Authentication	Not Implemented
IR-1	Incident response program established to restore systems and operations based on their criticality and within time constraints and effect recovery in case of a catalogue of disruptive events.	Priority 2 Controls	AWWA G430-14: 4.11 Emergency Response and Recovery Plans and Business Continuity Plans DHS CAT: 2.12.16 Control System Backup NIST 800-61R2: Whole Document	Not Implemented
MA-3	Off-site equipment maintenance program including risk assessment of outside environmental conditions established.	Priority 2 Controls	ISO/IEC 27001: Annex A: A.11.2.6 Security of equipment and assets off-premises NIST 800-53: Appendix F-SA: SA-9 External Information System Services	Partially Implemented
PM-3	Centralized logging system including policies and procedures to collect, analyze and report to management.	Priority 2 Controls	ISO/IEC 27002: 27002 15.3 Information Systems Audit Considerations NIST 800-53: Appendix F-AU: AU-6 Audit Review, Analysis, and Reporting	Not Implemented
PM-4	SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.	Priority 2 Controls	ISO/IEC 27001: Annex A: A.6.2.3 Addressing security in third party agreements NIST 800-124: 4.1 Security for the Enterprise Mobile Device Solution Life Cycle - Initiation NIST 800-53: Appendix F-SA: SA-9 External Information System Services	Not Implemented
RA-1	Risk assessment and approval process before granting access to the organization's information systems.	Priority 2 Controls	NIST 800-53: Appendix F-SI: SI-5 Security Alerts, Advisories, and Directives	Partially Implemented
RA-2	Third party agreement process to ensure that external vendors and contractors utilize appropriate security measures for access, processing, communicating, or managing the organization's information or facilities.	Priority 2 Controls	NIST 800-53: 2.5 External Service Providers NIST 800-53: Appendix F-SA: SA-9 External Information System Services	Not Implemented
SC-10	Program for hardening servers workstations routers, and other systems using levels of hardening based on criticality established. Program should include policies and procedures for whitelisting (deny-all, allow by exception).	Priority 2 Controls	NIST 800-34: 3.2 Conduct the Business Impact Analysis NIST 800-53: Appendix F-CM: CM-6 Configuration Settings	Not Implemented
SC-13	Testing standards including test data selection, protection, and system verification established to ensure system completeness.	Priority 2 Controls	NIST 800-53: Appendix F-SA: SA-11 Developer Security Testing and Evaluation	Not Implemented

ID	Priority	Description	References	Status
SC-4	Priority 2 Controls	Intrusion detection, prevention, and recovery systems including approved policies and procedures established to protect against cyber-attacks. System includes repository of fault logging, analysis, and appropriate actions taken.	NIST 800-53: Appendix F-SI: SI-4 Information System Monitoring	Not Implemented
SC-5	Priority 2 Controls	Anomaly based IDS/IPS established including policies and procedures.	NIST 800-53: Appendix F-SI: SI-4 Information System Monitoring	Not Implemented
SC-6	Priority 2 Controls	Network management and monitoring established including deep packet inspection of traffic, QoS, port-level security, and approved policies and procedures.	NIST 800-82r2: 5.6 Recommended Defense-in-Depth Architecture	Not Implemented
SC-7	Priority 2 Controls	Information exchange protection program in place to protect data in-transit through any communication system including the Internet, email, and text messaging and approved policies and procedures.	DHS CAT: 2.9.5 Information Exchange NIST 800-53: Appendix F-AC: AC-21 Information Sharing	Not Implemented
SC-8	Priority 2 Controls	Routing controls established to provide logical separation of sensitive systems and enforce the organization's access control policy.	DHS DID: 3.1.1 Architectural Zones ISA 62443-1-1: 5.8 Security Zones ISA 62443-3-3: 9.3 Network Segmentation NIST 800-82r2: 5.4 Logically Separated Control Network	Not Implemented
SC-9	Priority 2 Controls	Process isolation established to provide a manual override "air gap" between highly sensitive systems and regular environments.	ISA 62443-3-3: 9.3.3 Physical Network Segmentation	Partially Implemented
SI-5	Priority 2 Controls	Privileged program controls established to restrict usage of utility programs that could reset passwords or override controls as well as IT audit tools that can modify or delete audit data.	DHS DID: 3.5.1 Log and Event Management NIST 800-53: Appendix F-IA: IA-2 Identification and Authentication	Not Implemented
AU-8	Priority 3 Controls	Template for the organization's confidentiality/non-disclosure agreements defined, reviewed, and approved periodically by management.	ISO/IEC 27001: Annex A: A.13.2.4 Confidentiality or non-disclosure agreements	Not Implemented
CM-1	Priority 3 Controls	Policies for defining business requirements including data validation and message authenticity established to ensure that new/upgraded systems contain appropriate security requirements and controls.	DHS CAT: 2.15.28 External Access Protections ISA 62443-1-1: 5.5 Threat-Risk Assessment	Not Implemented
CM-2	Priority 3 Controls	Procedure modification tracking program in place to manage and log changes to policies and procedures.	ISO/IEC 27001: Annex A: A.5.1.2 Review of the policies for information security NIST 800-53: Appendix G: PM-1 Information Security Program Plan	Not Implemented
CM-4	Priority 3 Controls	Separation of duties implemented for development, production, and testing work.	ISO/IEC 27001: Annex A: A.6.1.2 Segregation of duties NIST 800-53: Appendix F-AC: AC-5 Separation of Duties	Not Implemented
IA-7	Priority 3 Controls	Wireless and guest-access framework established for the management, monitoring, review, and audit of wireless and guest access in place.	DHS CAT: 2.15.26 Wireless Access Restrictions DHS DID: 3 Isolating and Protecting Assets: Defense-in-Depth Strategies ISA 62443-3-3: 5.8 Wireless access management	Partially Implemented
IA-8	Priority 3 Controls	Policies for security of standalone, lost, and misplaced equipment in place.	ISO/IEC 27001: Annex A: A.11.2.1 Equipment siting and protection NIST 800-53: Appendix F-PE: PE-15 Water Damage Protection	Partially Implemented
IR-3	Priority 3 Controls	A legal/contractual/regulatory framework established to track legal/contractual/regulatory requirements and the efforts to meet them with respect to each important system within the organization. Another purpose of the framework is to ensure compliance of policies and procedures with privacy laws, handling cryptographic products, intellectual property rights, and data retention requirements.	DHS CAT: 2.9.7 Information and Document Retrieval	Not Applicable
MP-2	Priority 3 Controls	Information exit mechanisms in place to prevent data, software leaving premises without authorization or logging.	ISO/IEC 27001: Annex A: A.8.3.1 Management of removable media NIST 800-53: Appendix F-MP: MP-1 Media Protection Policy and Procedures	Not Implemented
PM-1	Priority 3 Controls	Asset management program including a repository containing all significant assets of the organization with a responsible party for each, periodic inventories, and audits.	ISA 62443-3-3: 11.1 Control system component inventory ISO/IEC 27001: Annex A: A.8 Asset Management NIST 800-53: Appendix F-CM: CM-8 Information System Component Inventory NIST 800-53: Appendix F-CM: CM-9 Configuration Management Plan	Partially Implemented
PM-2	Priority 3 Controls	Policies and procedures for acceptable use of assets and information approved and implemented.	ISO/IEC 27001: Annex A: A.8.1.1 Inventory of Assets NIST 800-53: Appendix G: PM-5 Information System Inventory	Partially Implemented
PS-1	Priority 3 Controls	Policies and procedures for hiring/terminating processes on employees, contractors, or support companies to include background checks and contract agreements approved and implemented.	DHS CAT: 2.3.1 Personnel Security Policy and Procedures	Partially Implemented
PS-2	Priority 3 Controls	Defined and approved security roles and responsibilities of all employees, contractors and third party users.	DHS CAT: 2.3.9 Personnel Roles	Partially Implemented
PS-3	Priority 3 Controls	A clear desk policy in place including clear papers, media, desktop, and computer screens.	DHS CAT: 2.3.8 Personnel Accountability ISO/IEC 27001: Annex A: A.11.2.9 Clear desk and clear screen policy ISO/IEC 27002: 27002 11.2.9 Clear desk and clear screen policy	Not Implemented

ID	Description	Priority	References	Status
PS-4	Disciplinary process for security violations established.	Priority 3 Controls	DHS CAT: 2.3.8 Personnel Accountability ISA 62443-2-1: A.3.3.2 Personnel security ISO/IEC 27001: Annex A: A.7.2.3 Disciplinary process	Not Implemented
SA-1	Authorization process established for new systems or changes to existing information processing systems.	Priority 3 Controls	ISO/IEC 27001: Annex A: A.14.2 Security in development and support processes NIST 800-53: Appendix G: PM-10 Security Authorization Process	Not Implemented
SA-2	Change controls of systems development, outsourced development, system modification, and testing established, including acceptance criteria for new systems, monitoring of internal/outsourced development, and control of system upgrades.	Priority 3 Controls	DHS CAT: 2.6.3 Configuration Change Control ISO/IEC 27001: Annex A: A.14.2.2 System change control procedures NIST 800-53: Appendix F-SA: SA-10 Developer Configuration Management	Not Implemented
SA-3	Change controls of operating systems, network configuration/topology, network security established, including changes to IDS/IPS, traffic control/monitoring, new systems, and system upgrades.	Priority 3 Controls	NIST 800-82r2: 6.2.5 Configuration Management	Not Implemented
SA-4	Risk based mobility policies and procedures established to protect against inherent risk of mobile computing and communication systems.	Priority 3 Controls	DHS CAT: 2.15.25 Access Control for Mobile Devices NIST 800-34: Executive Summary	Not Implemented
SA-5	Periodic review of backup policies and procedures and testing of recovery processes.	Priority 3 Controls	ISO/IEC 27001: Annex A: A.14.2.3 Technical review of applications after operating platform changes NIST 800-53: Appendix F-CM: CM-3 Configuration Change Control	Not Implemented
SI-2	System acceptance standards including data validation (input/output), message authenticity, and system integrity established to detect information corruption during processing.	Priority 3 Controls	DHS CAT: 2.5 System and Services Acquisition ISO/IEC 27001: Annex A: A.14.2.9 System acceptance testing	Not Implemented
SI-4	Organization-wide clock synchronization system in place.	Priority 3 Controls	NIST 800-53: Appendix F-AU: AU-8 Time Stamps	Not Implemented
CM-6	Risk based policies and procedures for change controls, reviews, and audits of SLAs.	Priority 4 Controls	ISO/IEC 27001: Annex A: A.14.2.2 System change control procedures NIST 800-53: Appendix F-CM: CM-1 Configuration Management Policy and Procedures	Not Implemented
IA-2	Access control for the management, monitoring, review, and audit of accounts established including access control, account roles, privilege accounts, password policies and executive oversight.	Priority 4 Controls	ISO/IEC 27001: Annex A: A.9.2.1 User registration and de-registration NIST 800-53: Appendix F-IA: IA-4 Identifier Management AWWA G430-14: 4.4 Up-to-Date Assessment of Risk	Not Implemented
IR-2	A security program established to respond to security incidents monitor, discover, and handle security alerts and technical vulnerabilities, collect and analyze security data, limit the organization's risk profile and ensure that management is aware of changing/emerging risks.	Priority 4 Controls	DHS CAT: 2.12 Incident Response NIST 800-61R2: Whole Document	Not Implemented
MA-1	Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity.	Priority 4 Controls	ISO/IEC 27001: Annex A: A.11.2.4 Equipment maintenance NIST 800-53: Appendix F-MA: MA-2 Controlled Maintenance	Partially Implemented
MA-2	Maintenance of relationships with authorities, professional associations, interest groups etc., formalized.	Priority 4 Controls	ISO/IEC 27001: Annex A: A.13.2.4 Confidentiality or non-disclosure agreements NIST 800-53: Appendix F-AC: AC-19 Access Control for Mobile Devices	Partially Implemented
MP-1	Storage media management and disposal program established to ensure that any sensitive data/software is used appropriately and is removed prior to media disposal (including approved policies and procedures).	Priority 4 Controls	DHS CAT: 2.13 Media protection NIST 800-53: Appendix F-MP: MP-6 Media Sanitization	Not Implemented
MP-3	Policies and procedure repository in place to be available to all authorized staff.	Priority 4 Controls	ISA 62443-2-1: A.3.2.6 Security Policies and Procedures NIST 800-53: Appendix G: PM-1 Information Security Program Plan	Partially Implemented
PM-5	Data classification policies and procedures for handling and labeling based on confidentiality and criticality approved and implemented.	Priority 4 Controls	ISO/IEC 27001: Annex A: A.8.2.1 Classification of Information NIST 800-53: Appendix F-RA: RA-2 Security Categorization	Not Implemented

Appendix K
AWWA CYBERSECURITY TOOL OUTPUT

WATER SECTOR CYBERSECURITY RISK MANAGEMENT GUIDANCE

Prepared by West Yost Associates

Tool and Guidance Revision History		
Version	**Date**	**Description**
1.0	4/4/2014	Initial Release
2.0	2/22/2017	Revised to match updated Cybersecurity Guidance tool. The Use Case descriptions were revised for clarity. Use cases were added to address wireless communications. An additional 12 cyber controls were added.
3.0	9/4/2019	Revised to improve user interface. Explicitly supports AWIA 2018 §2013 compliance. Updates to the use cases and controls, and alignment with NIST Cybersecurity Framework v1.1. Provide Microsoft Excel-based output to allow for self-assessment of controls and development of an improvement plan.

Disclaimer

The authors, contributors, editors, and publisher do not assume responsibility for the validity of the content or any consequences of its use. In no event will AWWA be liable for direct, indirect, special, incidental or consequential damages arising out of the use of information presented herein. In particular, AWWA will not be responsible for any costs, including, but not limited to, those incurred as a result of lost revenue.

CONTENTS

ACKNOWLEDGEMENTS

Project Advisory Committee

- Norm Anderson, Carollo Engineers
- John Brosnan, Santa Clara Valley Water District
- Don Dickinson, Phoenix Contact
- Patrick Norton, Tampa Bay Water
- Robert Raffaele, American Water

Project Contractors

- Andrew Ohrt, West Yost Associates
- Dan Groves, West Yost Associates
- Jeff Pelz, West Yost Associates
- Joel Cox, West Yost Associates
- Murphy Altunel, West Yost Associates
- Bailey Bartolucci, West Yost Associates
- Judith H. Germano, GermanoLaw LLC
- Gwen M. Schoenfeld, GermanoLaw LLC
- Gemma Kite, Horsley Witten Group, Inc.
- Tom Noble, Horsley Witten Group, Inc.
- Will Keefer, Horsley Witten Group, Inc.

Subject Matter Expert Panel

- Danielle Anderson, City of Minneapolis Water Treatment and Distribution Services Division
- Will Bianchini, Onondaga County Water Authority
- Andy Bochman, Idaho National Laboratory
- Jacques Brados, Black and Veatch
- Geoffrey Brown, Alameda County Water District
- Bernie Bullert, SL-Serco
- Travis Cochrane, City of Corpus Christi
- Jeff Cooley, City of Vacaville Public Utilities
- Steve Crumley, City of Minneapolis Water Treatment and Distribution Services Division
- Charley Cunningham, City of Sacramento Department of Utilities
- Bob Daly, EMA Inc.
- Jon Eaton, City of Eagan Public Utilities
- Bill Fisher, National Institute of Standards and Technology
- Jamie Foreman, City of Carmel Public Works
- Glen Goins, The Automation Group
- Andrew Hildick-Smith, Massachusetts Water Resource Authority
- Daniel Honore, Village of Pleasant Prairie Utility Department
- Dr. Connie Justice, Indiana University Purdue University Indianapolis
- Marlene Ladendorff, Schneider Electric
- Michael Lewis, City of Albany Public Works
- Jim Livermore, CDM Smith
- Mike Malone, Eastern Municipal Water District
- Blas Moreno, Prince William County Service Authority
- Ariz Naqvi, Alameda County Water District
- Debbie Newberry, United States Environmental Protection Agency
- Janine Nielsen, Rockwell Automation, Inc.
- Kevin Owens, Control Cyber Inc.
- Cayce Parrish, United States Environmental Protection Agency
- David Paul, AquaEngineers
- Chuck Redding, City of Sacramento Department of Utilities
- Nelson Sims, DC Water and Sewer Authority
- Chris Walcutt, Black and Veatch
- Jennifer Lyn Walker, WaterISAC
- Linda Warren, Launch! Consulting

Acronym and Abbreviation Table

Acronym /Abbreviation	Description
ANSI	American National Standards Institute
AWIA 2018	America's Water Infrastructure Act of 2018
AWWA	American Water Works Association
CCE	Consequence-Centered Engineering
CFR	Code of Federal Regulations
CIA	Confidentiality Integrity and Availability
CIA	Confidentiality, Integrity, and Availability
CIE	Cyber-Informed Engineering
CIR	Committed Information Rate
CISSP	Certified Information Systems Security Professional
ERP	Emergency Response Planning
FOIA	Freedom of Information Act
HIPAA	Health Insurance Portability and Accountability Act
INL	Idaho National Laboratory
ISA	International Society of Automation
IT	Information Technology
LAN	Local Area Network
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OPSEC	Operations Security
PCI	Payment Card Industry
PCS	Process Control Systems
PII	Personally identifiable information
PLC	Programmable Logic Controller
QoS	Quality of Service
RRA	Risk and Resilience Assessment
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SME	Subject Matter Experts
SSN	Single Sign On
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WITAF	Water Industry Technical Action Fund

EXECUTIVE SUMMARY

Within the last several decades, cybersecurity threats, including such things as cyber-terrorism and ransomware attacks, have grown from the esoteric practice of a few specialists to a problem of general concern. Critical infrastructure systems serving the people of the United States have been found to be particularly vulnerable to such attacks. As noted in the Cybersecurity Risk and Responsibility in the Water Sector[1]:

"Government intelligence confirms the water and wastewater sector is under a direct threat as part of a foreign government's multi-stage intrusion campaign, and individual criminal actors and groups threaten the security of our nation's water and wastewater systems' operations and data."

In response to the general threat to critical infrastructure, a wide array of standards and guidelines are available to assist organizations with implementing security controls to mitigate the risk from cyber-attacks. The scope of these documents is large, and the security controls in the standards often require significant planning and years of implementation.

In February 2013, the American Water Works Association (AWWA) Water Utility Council initiated a project (WITAF #503) to address the absence of practical, step-by-step guidance for protecting water sector process control systems (PCS)[2] from cyber-attacks. This action was timely as it corresponded with the development of the National Institute of Standards and Technology (NIST) Cybersecurity Framework as called for in Executive Order 13636 - Improving Critical Infrastructure Cybersecurity.[3] The NIST Cybersecurity Framework includes a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

This AWWA Water Sector Cybersecurity Risk Management Guidance (AWWA Guidance) and associated AWWA Cybersecurity Assessment Tool (AWWA Assessment Tool), collectively referred to as AWWA Guidance and Assessment Tool, is a voluntary, sector-specific approach for adopting the NIST Cybersecurity Framework as expressed by the Water Sector Coordinating Council. The original goal of this AWWA guidance was to provide water sector utility owners/operators with a consistent and repeatable assessment tool and recommended course of action to reduce vulnerabilities to cyber-attacks as recommended in ANSI/AWWA G430: Security Practices for Operations and Management and EO 13636. The guidance is also expected to communicate a "call to action" for utility executives acknowledging the significance of securing PCS and enterprise systems (e.g. information technology) given their role in supporting water utility operations.

This AWWA Guidance and Assessment Tool update was developed to assist community water systems (i.e. utility) in complying with section 2013 of America's Water Infrastructure Act (AWIA) of 2018 (PL 115-270).[4] AWIA requires all community water systems serving populations of 3,300 or more to conduct and certify completion of an assessment of the risks to, and resilience of their systems, including an emergency response plan. The new requirement places emphasis on assessing and mitigating cybersecurity risks that could impact the following:

- Electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;

---

[1] American Water Works Association, *Cybersecurity Risk and Responsibility in the Water Sector*, 2018.

[2] The term process control system (PCS) is preferred over industrial control system (ICS) to avoid confusion with incident command system (ICS) common in national emergency response planning.

[3] Executive Order 13636 - Improving Critical Infrastructure Cybersecurity, https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

[4] The text of AWIA §2013 is included in Appendix A.

- The monitoring practices of the system (including network monitoring); and
- The financial infrastructure of the system (accounting and financial business systems operated by a utility, such as customer billing and payment systems).

Utilities may have PCS and enterprise systems that are physically or logically connected. In addition, many business applications that utilities rely on to support critical day-to-day operations reside within enterprise systems. To account for this, enterprise systems are explicitly included in the AWIA requirements for the risk and resilience assessment (RRA) and emergency response plan (ERP).

A panel of subject matter experts was consulted to identify the most pressing cybersecurity issues facing water utilities today. In response to these issues, a recommended grouping of cybersecurity practices was developed. This grouping identifies cybersecurity practice areas considered to be the most critical for managing cyber risk in the water sector. This guidance provides a discussion of the recommended practice areas and why they are important to supporting a robust cybersecurity risk management strategy.

These recommended practices are defined by a set of 99 cybersecurity controls that are organized in a manner to facilitate implementation based on actionable tasks. The outputs of the AWWA Assessment Tool are designed to present these controls to users in a concise, straightforward manner, facilitate documentation and support future compliance actions and improvement.

The AWWA Assessment Tool generates a prioritized list of recommended controls based on specific characteristics of the utility. The user provides information about the manner in which their PCS and enterprise systems are used. Based on these practices, use cases are selected to recommend controls. For each recommended control, specific references to existing cybersecurity standards are also provided.

The AWWA Assessment Tool emphasizes actionable recommendations with the highest priority assigned to those that are expected to provide the greatest impact in the short term. It should be noted, however, that the tool does not assess the extent to which a utility has implemented any of the recommended controls. This is the responsibility of the utility. To facilitate this, additional tool outputs were added and are discussed in the following sections.

This resource is a living document, and further revisions and enhancements will be made based on the quickly evolving cyber-threat landscape and user feedback.

Use of this Guidance to Support AWIA §2013 Compliance

As noted above, one objective of the AWWA Cybersecurity Guidance and Assessment Tool is to support utilities with AWIA §2013 compliance actions. Additional guidance is provided in subsequent sections of this document.

Utility staff responsible for AWIA §2013 compliance may not be cybersecurity technologists or responsible for the secure and reliable operation of the PCS and/or enterprise systems. Therefore, it is recommended that a utility convene internal and external support staff, including, but not limited to:

- Utility compliance staff responsible for AWIA §2013 compliance.

- Utility staff responsible for and knowledgeable of the design, operation, and maintenance of the utility's PCS and enterprise systems (information technology).
- Utility leadership responsible for overall operation of the utility (utility staff with the authority to accept risks should be present).
- External support staff including cybersecurity vendors, engineering firms, etc., if needed.

This approach will improve the quality and timeliness of data collection. In addition, it is expected to reduce the overall time required to complete compliance actions while also improving the cybersecurity posture[5] of the organization.

Cybersecurity Guidance and Tool Output Information Security

The output of the Assessment Tool should be classified as critical infrastructure security information. In many states, this means that it is protected from public informaton requests. To maintain a high level of information security after the output is generated, AWWA strongly recommends the following:

- If your utility has a data classification system in place, treat the output and associated information as the most protected type of information. It is recommended that this be done with consideration to the FOIA/sunshine laws in your jurisdiction.
- If your utility does not have a data classification system in place:
  - Store this data in a secure location.
  - Restrict access to this information as much as possible. For example: do not email this document.

RECOMMENDED CYBERSECURITY PRACTICES

Overview

These practices are comprised of recommendations to improve the cybersecurity posture of water and wastewater utilities. They are actionable recommendations designed to produce maximum improvement in the short term and provide a foundation for longer term implementation of a comprehensive cybersecurity risk management strategy.

The terminology used within this section and other standards is fundamentally technical. AWWA strived to make the guidance and user experience as "plain English" as possible. However, some additional insight into the networking and network component terminology may be helpful to the reader. It is recommended that the reader refer to Appendix B: Network Architecture Reference Diagram and Definitions.

Practice Categories

The practice categories were chosen by Subject Matter Experts (SME) teams during a Definition Workshop. Each team identified important areas of cybersecurity to be addressed and policies, activities, and systems that should be implemented. The recommendations from the SMEs were collected, integrated (to avoid duplication), and loosely organized into the ten domains of the Certified Information Systems Security Professional (CISSP) Common Book of Knowledge. Several reviews and additions followed until there was consensus that the practives categories and recommendations were comprehensive. The categories (like their NIST framework counterparts) are not mutually exclusive and contain significant overlap. In addition, the AWWA Assessment Tool output categorizes the

---

[5] The cumulative strength of a utility's cybersecurity policies, controls, and how effectively they mitigate risk.

recommended controls into these practice areas. The following is a description of each practice category.

Governance and Risk Management

This category is concerned with the management and executive control of the security systems of the organization; it is associated with defining organizational boundaries and establishing a framework of security policies, procedures, and systems to manage the confidentiality, integrity, and availability (CIA) of the organization. One of the key components of system governance is developing and maintaining an accurate, up-to-date inventory of PCS and enterprise system components.

Cyber supply chain risk management is an important component in the design, operation, and maintenance of PCS and enterprise systems. This includes such things as establishing cybersecurity requirements for suppliers, communication of these requirements, and verifying the requirements are met.

From the perspective of long-term security, this is the most important category because it creates a managed process for increasing security. It also engages the executive team by including security risks as an important part of enterprise risk management.

Although this category of recommendations represents an essential part of an organization's security posture, the related cybersecurity controls have been assigned a slightly lower priority in order to emphasize actionable recommendations that can have significant short-term effects.

Business Continuity and Disaster Recovery

This category is concerned with ensuring that the control system continues running even when faults occur and with rapid recovery after a service disruption.

Business Continuity Planning is a structured method for an organization to prepare for and reduce the probability and impact of systems and operational failure. A key component of Business Continuity Planning is the Disaster Recovery Plan, which deals with longer disruptions from more impactful events.

Both plans require a managed process that identifies potentially disruptive events, estimates their impact, and then develops and monitors mitigation strategies.

Server and Workstation Hardening

This category is concerned with securing servers and workstations against cyber-attacks; it identifies best practices to minimize the probability of unauthorized access to servers, and to maintain the CIA properties of the servers and the systems within them. For example, this category includes whitelisting, which restricts the applications that are permitted to run on servers and workstations throughout the enterprise.

Access Control

This category is concerned with ensuring that only authorized personnel are permitted to access computing resources within the organization; it pertains to best practices for restricting access to computing resources and information to authorized users. For example, Single Sign On (SSN) is an access control mechanism that requires users to sign on only once; the SSN system can then use those credentials to control access to a variety of applications. However, care should be taken to ensure that different passwords are used to access PCS and enterprise systems.

Application Security

This category is concerned with ensuring that computer programs do only what they are supposed to do; for example, suppose that a module of a Supervisory Control And Data Acquisition (SCADA) system is supposed to receive data from a Programmable Logic Controller (PLC) and save it. Application security

contains best practices to ensure that the module is not susceptible to buffer-overflow attacks and that the data it receives does not get corrupted as it is handled by the module.

Application Security is a complex and extensive area involving the design, implementation, and testing of program modules as well as the testing and monitoring of integrated systems after implementation. Utilities should develop standard design and implementation requirements that define the testing required by software vendors and system integrators, as well as doing their own testing of the integrity of results.

Encryption

This category is concerned with ensuring that only appropriate encryption schemes are used within an organization's security systems and that the cryptography is used wherever it is needed. For example, there is general confusion of what is an appropriate encryption scheme: sometimes packing or compression algorithms are called encryption. Also, cryptographic systems must be used wherever they are needed, for example, if the data will be traveling on a public channel or via a wireless circuit, or if there is a need to provide non-repudiation of a message or a document (by using a cryptographic signature).

Weak encryption schemes are particularly dangerous because they provide little protection and create a false sense of security and complacency. Proprietary encryption schemes should be avoided since they typically have not gone through comprehensive testing and often contain flaws. Also, only encryption schemes that are referenced by appropriate standards and use keys of proper length should be considered secure.

Data Security

This category is concerned with various types of protected data that a utility may collect, transfer and store. This includes payment information like credit and debit cards, personally identifiable information (PII), and health information protected according to Health Insurance Portability and Accountability (HIPAA) requirements. These requirements are included in this category.

Telecommunications, Network Security, and Architecture

This category is concerned with the security of the network infrastructure from the data connector on the wall to the enterprise switches, routers, and firewalls. This includes the physical security of the cables, the telecom closets, and the computer rooms, and the protection of the data as it travels on public channels and wireless circuits. Spam filtering and website blocking are also included in this category.

The focus of this category is establishing a "defense-in-depth" network architecture with the network at its core. It also addresses adherence to new standards for PCS network security, particularly network topology requirements within the vicinity of PCS systems and PLC controls. Another area addressed in this category is network management, including port level security.

Physical Security of PCS Equipment

Physical security is a basic requirement for all PCS and enterprise systems. Once physical access to a network device or server is achieved, compromising equipment or systems is usually a trivial matter. The recommended practices in this category focus on preventing and restricting physical access to only authorized personnel with a need to perform some action on the hardware. The recommendations in this group are also related to monitoring, detecting, and responding to unauthorized physical access.

Service Level Agreements (SLA)

This category is concerned with the definition and management of contracts that specify services requirements to the organization. The contract manager under the direction of the executive team is

responsible for defining, negotiating, executing, and monitoring these contracts to ensure appropriate service delivery to the organization.

An SLA is a contract which requires minimum levels of performance for services provided. For example, the Committed Information Rate (CIR) is part of a typical Wide-Area Network (WAN) SLA and specifies the minimum bandwidth that a data circuit may have.

SLAs for PCS network systems typically focus on quality of service (QoS) rather than bandwidth. PCS systems do not require high bandwidth but cannot operate properly if the bandwidth falls below certain known thresholds. Conversely, SLAs for enterprise systems will focus on confidentiality and integrity of information stored or in transit on the network.

Operations Security (OPSEC)

OPSEC is concerned with refining operational procedures and workflows to increase the security properties (CIA) of an organization. For example, a utility may want to restrict what employees post on their social media pages about the organization's security procedures. OPSEC also includes access granting policies and procedures, security guard rotation schedules, backup recovery procedures, etc.

Education

This category is concerned with bringing security awareness to the employees, clients, and service providers of the organization.

Education involves identifying best practices and providing formal training on the security policies and procedures of the enterprise as well as security awareness and incident response. It involves test practice of the key security processes and actions to ensure quick and accurate response to security incidents within the enterprise.

Personnel Security

This category is concerned with the personal safety of employees, clients, contractors, and the general public. Personnel security starts as part of the hiring process and ends after the employee leaves the organization. It handles periodic reaccreditation of employees and updates of the policies and procedures that govern staff. The purpose of personnel security is to ensure the safety and integrity of staff within the organization. Personnel security also applies to external contractors and service personnel, with the objective to ensure appropriate, lower privileged access to facilities.

Cyber-Informed Engineering

Cyber-Informed Engineering (CIE)[6,7] and the associated Consequence-Centered, Cyber-Informed Engineering (CCE)[8] are methodologies recently developed and promulgated by Idaho National Laboratory (INL). The methodologies emphasize the integration of cyber risk considerations into the full engineering life-cycle to reduce risk. These approaches recognize that, while extremely important, a cyber-hygiene centered approach cannot address the rapidly evolving cyber threats that all critical infrastructure owners and operators face. Therefore, utilities need to take additional measures to ensure that their systems are cyber-resilient.

---

[6]Anderson, Robert S., Benjamin, Jacob, Wright, Virginia L., Quinones, Luis, and Paz, Jonathan. Cyber-Informed Engineering. United States: N. p., 2017. Web. https://doi.org/10.2172/1369373

[7]Wright, Virginia. Cyber-Informed Engineering. Fermilab Colloquium. September 21, 2016. https://vms.fnal.gov/asset/detail?recid=1944478&recid=1944478

[8] Bochman, Andy. The End of Cybersecurity. Harvard Business Review. May 2018.

CYBERSECURITY TOOL USER GUIDANCE

Overview

The Assessment Tool uses several steps to collect user input on the utility's current cybersecurity posture and provides recommended controls to facilitate AWIA §2013 compliance and cybersecurity improvements. PLEASE NOTE: AWWA DOES NOT COLLECT ANY DATA ENTERED INTO THE TOOL OR ABOUT USERS OF THE TOOL. Rather, this guidance and the Assessment Tool provide the user with recommended controls based on how the utility describes the application of certain technologies and practices in their day-to-day operations. No security sensitive information is required or shared by the user. The process flow of the tool is segmented to address the two primary phases of AWIA §2013, 1) Risk and Resilience Assessment (RRA; dark blue box) and 2) Emergency Response Planning (ERP; green box), is illustrated in Figure 1.
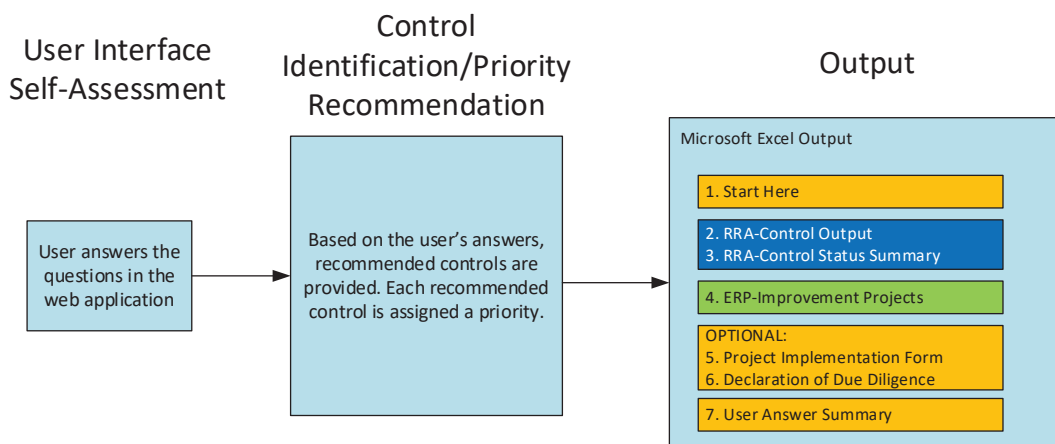
Figure 1. AWWA Cybersecurity Tool Process

The following sections provide additional detail on the individual inputs, processing steps, and outputs of the AWWA Assessment Tool.

User Interface

First, the user answers questions on the policies, procedures and use of their PCS and enterprise systems in the web application. The AWWA Assessment Tool automatically maps the utility's PCS and enterprise system configuration and practices to the recommended control. The questions designed to capture the utility's PCS and enterprise system configuration and practices are included in a worksheet format in Appendix C of this guidance.

Use-Cases

A use-case is an elemental pattern of behavior as described by the user of a system; the use-cases in this document are basic descriptions of important processes from the user's perspective. Based on the use-cases selected, the tool provides recommended cybersecurity controls. Appendix D includes a table

summarizing the use-cases included in the tool. These are no longer visible to the user, but were retained to maintain consistent mapping of controls.

Cybersecurity Controls

A security control is a measure to support effective cyber defense. Most of the controls in this document are measures designed to reduce risk; they were developed from many industry standards which were correlated, integrated, and enhanced. For example, multiple similar controls were merged into a single, more comprehensive control. Some controls are complex and might resemble an administrative program, a computer system, or an engineering design methodology. Many cybersecurity service vendors provide computer systems to implement controls of greater complexity (e.g., network monitoring tools). Appendix E provides a list of the cybersecurity controls developed for this document and a table mapping the controls presented in Appendix E to the controls presented in the NIST Cybersecurity Framework v1.1 is included as Appendix F.

Each control was assigned a priority level based on its criticality and potential impact to the security of the utility. The recommended controls are categorized into priorities 1, 2, 3, and 4, with priority 1 being the highest. For each recommended control, a reference is provided to a set of existing cybersecurity standards. Priority levels are adapted from SANS[9] and are defined as follows:

- **Priority 1 Controls** – These controls represent the minimum level of acceptable security for PCS and enterprise systems. If not already in place, these controls should be implemented immediately. In some cases, they could be considered q*uick wins* that provide solid risk reduction without major procedural, architectural, or technical changes to an environment. Alternatively, a control may provide substantial and immediate risk reduction against common attacks. Generally, these will be cyber-hygiene measures. Utilities with many Priority 1 controls to implement will likely be reactive to any cyber-attack.

- **Priority 2 Controls** – These controls build on those in the Priority 1 category. Despite being Priority 2, these controls have the potential to provide a significant and immediate increase in the security of the organization. Generally, these will be more sophisticated cyber-hygiene measures to improve the process, architecture, and technical capabilities of the utility. These improvements include capabilities such as monitoring of networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

- **Priority 3 Controls** – These controls improve information security configuration and hygiene to reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage. These controls lay the foundation for sustained implementation of a managed security system. These controls include

---

[9] SANS. CIS Critical Security Controls: Guidelines. https://www.sans.org/critical-security-controls/guidelines. Last accessed May 1, 2019.

more sophisticated longer-term approaches to managing cyber-risk including CIE and cyber supply chain risk management.

- **Priority 4 Controls** – These controls are more complex and provide proactive protection against more sophisticated attacks. These include new technologies, policies, and methods that provide maximum security but are more complex and potentially more expensive than commoditized security solutions.

Maturity is a concept that is widely used in other sectors. Generally, the maturity of an organization's cybersecurity posture is the extent to which a utility has implemented the recommended controls. It is also reflective of a utility moving from a *reactive* to a *proactive* cybersecurity posture. Adapted from SANS,[10] Figure 2 illustrates notional levels of maturity.
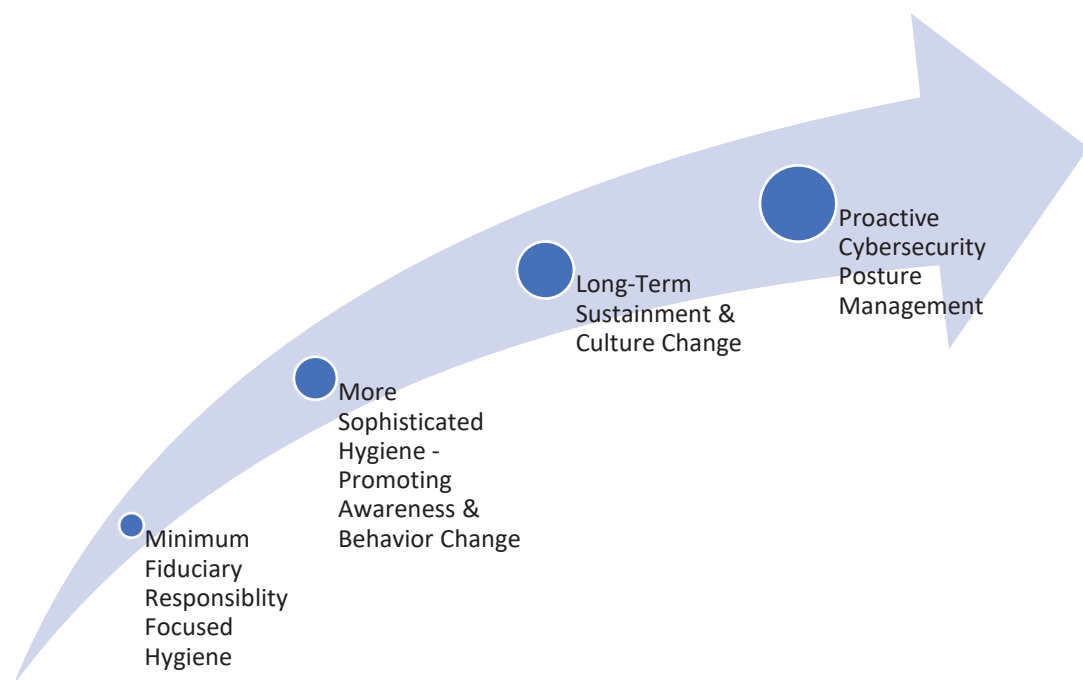
Figure 2. Conceptual Cybersecurity Maturity Levels of an Organization

The maturity levels in Figure 2 are comparable to Tiers 1 through 4 in the NIST Cybersecurity Framework. The Tiers range from Tier 1 – Partial to Tier 4 - Adaptive. The Tiers describe the degree to which a utility's cybersecurity risk management practices exhibit the characteristics defined in the NIST Cybersecurity Framework.[11]

Using this guidance and the Assessment Tool, utilities should assess the controls in place and their associated implementation status (i.e. maturity) on a recurring basis relative to the current and anticipated needs of the organization, the current cybersecurity posture of the organization, and the

---

[10] SANS.org. https://www.sans.org/sites/default/files/10_24%20Blog%203%20Commandments.png. Last accessed May 1, 2019.

[11] NIST Cybersecurity Framework. An Introduction to the Components of the Framework. https://www.nist.gov/cyberframework/online-learning/components-framework. Last accessed May 28, 2019.

threat landscape. Broadly, the objective should be to continuously move from the minimum controls in place for fiduciary responsibility and a reactive posture to a proactive posture.

Recommended Cybersecurity Practices and Improvement Projects

Each Practice Category identified in has numerous associated recommended controls and potential improvement projects. Some additional details on potential improvement projects are provided below:

1. **Governance and Risk Management**
    a. Develop a formal, written Cybersecurity Policy that addresses the specific operational needs of PCS and enterprise systems.
    b. Establish an Enterprise Risk Management strategy that associates cybersecurity investments with enterprise business plans.
    c. Perform a vulnerability assessment (e.g. CSET or physical assessment) on a regular basis.
    d. To aid in developing contingency plans, maintain current network asset inventory, baseline, "gold disk," including:
        i. Applications
        ii. Data
        iii. Servers
        iv. Workstations/HMI
        v. Field devices (e.g. PLCs)
        vi. Communications and network equipment
    e. Develop and enforce hardware and software standards in order to limit number of system components
    f. Develop standard specifications language that defines cybersecurity standards for inclusion in all procurement packages for PCS and enterprise systems

2. **Business Continuity and Disaster Recovery**
    a. Develop resilience plans including: Emergency Response Plan, Continuity of Operations Plan, and/or Disaster Recovery/Business Continuity Plan. These plans should include:
        i. Crisis Management Team (including at least one representative from executive management) – with authority to declare an alert or a disaster and who monitors and coordinates the necessary recovery activities.
        ii. Manual overrides to allow temporary manual operations of key processes during an outage or a cyber-attack.
        iii. Strategies for system redundancy (or offline standby) to ensure key system components can be restored within acceptable timeframes.
    b. Ensure that corporate Emergency Response Plan, Continuity of Operations Plan, and/or Disaster Recovery/Business Continuity Plan includes procedures and contact list for PCS and enterprise systems.
    c. Conduct exercises to test and revise plans and build organizational response capabilities.

d. Implement change management program for PLC software; maintain fully commented backups for all PLC programs and test restore process on a periodic basis.

e. Implement change management program for enterprise systems with routine backups and restoration exercises.

f. Test backup and recovery plans regularly.

3. **Server and Workstation Hardening**

a. Implement whitelisting (allows only specified applications to execute on each specific computer).

b. Maintain support contracts with HMI software vendor and implement antivirus, anti-malware, and operating system patches in accordance with vendor's direction.

c. Implement security patch management program with periodic vulnerability scanning.

d. Implement change management program for applications and infrastructure (routers, etc.)

e. Harden critical servers and workstations.

f. Remove local administrator rights, delete/disable default accounts (OS and application).

g. Rename Administrator account.

h. Disable USB, DVD, and other external media ports.

i. Disable auto-scan of removable media.

4. **Access Control**

a. Secure PCS and enterprise system access.
    i. Physical access to facilities and equipment.
    ii. Application access to key software functions.
    iii. External access should be controlled. Address requirements for:
        1. File exchange into or out of a network. Include system and software updates.
        2. Data exchange between PCS and enterprise systems such as email (alarms), historical databases, CMMS, LIMS, etc.
        3. Establish off-line or isolated system for testing and patch management, including applications and device programs.
        4. Identify what is required for remote access. Restrict remote access to lowest level of privilege required.
    iv. Vendor, contractor system access on plant (incl. package systems). Vendor or contractor access to system should be manually initiated.
    v. Equipment (e.g. network equipment, field devices) access

b. Secure remote access
    i. Use VPN technologies to protect information in transit.
    ii. Require multifactor authentication (e.g. tokens) for remote access to sensitive functions.
    iii. Limit access to only the minimal level required (e.g. view-only web page).

    c.   Implement multi-factor authentication for all workstations.

    d.   Laptops that are used to control PCS or program field devices should be "dedicated for PCS use only" and ports to Internet disabled. All non-essential software should be removed.

5. Application Security

    a.   Require each PCS or enterprise system user to utilize unique credentials (usernames and passwords) which provide only the required level of access needed to perform their job. Establish policy for strength of password and periodic renewal. Implement automatic lock out after adjustable number of failed log-in attempts.

    b.   Provide separate accounts for administrator and user functions. Do not allow users to operate with administrator rights unless they are actually administering the system.

    c.   Provide separate credentials for PCS access compared to enterprise system access. Require different passwords between systems.

    d.   Implement audit controls such as logging and monitoring of system access and modification.

    e.   Aggregate system logs and conduct frequent review of network, application and systems events.

6. Encryption

    a.   Implement device and/or storage encryption where theft or loss of a device is a possibility:

        i.   Smartphones, tablets containing sensitive system information.

        ii.   Laptops containing programs or other sensitive information.

        iii.   Equipment (e.g. administrator passwords).

        iv.   Removable media (e.g. tape, disk, USB removable storage).

    b.   Implement communications encryption:

        i.   Wireless communications should be encrypted where possible, regardless of type or range.

        ii.   Wired communications over shared infrastructure (e.g. leased, shared) should be encrypted using VPN technologies to protect sensitive information in transit.

    c.   Implement "best available" encryption.

        i.   Use strongest available encryption on existing equipment.

        ii.   Identify encryption requirements in specifications for new equipment.

    d.   Implement encryption of confidential data in on-line repositories.

7. Data Security

    a.   Implement appropriate measures to accept, process, store, and/or transmit customer billing information. The Payment Card Industry (PCI) priorities include:

        i.   Remove sensitive authentication data and limit data retention.

        ii.   Protect systems and networks, and be prepared to respond to a system breach.

        iii.   Secure payment card applications.

        iv.   Monitor and control access to your systems.

v. Protect stored cardholder data.

vi. Finalize remaining compliance efforts, and ensure all controls are in place.

b. Implement controls to protect Personally Identifiable Information (PII)

i. Understand how PII is defined based on local, state, and federal statutes

ii. Develop a privacy policy.

iii. Develop a data breach response policy.

c. Implement controls to achieve and maintain HIPAA compliance

i. Establish a program to maintain minimal compliance with HIPAA requirements.

ii. Develop a privacy policy.

iii. Develop a data breach response policy.

8. **Telecommunications, Network Security, and Architecture**

a. Implement Layered Network Security with multiple levels of protection

i. Utilize stateful or application layer firewalls, filtering routers, packet filtering or similar devices between networks.

ii. Implement Intrusion Detection/Prevention Systems to identify and alarm on or block unauthorized access.

iii. Implement security information and event management (SIEM)/anomaly detection to provide real-time monitoring of all PCS equipment and enterprise systems.

b. Implement network separation

i. Implement physical (e.g. dedicated hardware) and/or logical separation (IP subnets, VLANs) to protect sensitive functions:

1. Between PCS, enterprise systems, and other networks.

2. Within PCS and enterprise systems:

a. Servers

b. HMI

c. Field equipment

d. Network management

e. Third party controlled equipment

3. Over shared communications equipment or links

c. Implement port-level security on all network devices.

d. Evaluate the risks and benefits of "pulling the plug" between PCS and the outside world.

e. Develop an architecture that will allow critical operations to continue if isolated.

f. Implement network management system to monitor system performance and identify potential bottlenecks.

g. Document and periodically review PCS network architecture and enterprise system network architecture (including definition of network boundaries).

9. **Physical Security of PCS Equipment**
   a. Control access to:
      i. Unused network ports
      ii. Removable media
      iii. Equipment cabinets and closets
      iv. Control room
      v. Facilities
      vi. Communications pathways

10. **Service Level Agreements**
    a. Identify all external dependencies and establish written Service Level Agreements and support contracts with internal and external support organizations to clearly identify expectations for response time and restoration of shared or leased network infrastructure and services, including equipment or services provided by:
       i. Equipment or service managed by IT departments
       ii. PCS vendors
       iii. Telecommunications and Internet providers
       iv. Power sources/power supply (within facilities)
       v. System vendors
       vi. System integrators
    b. Leverage procurement policies to limit number of external support organizations.
    c. Establish SLA's with staff and contracted employees for responsiveness and agreement to respond in emergency conditions.

11. **Operations Security (OPSEC)**
    a. Provide clear demarcation between business and PCS functions. Isolate all non-PCS functions and block access from PCS equipment to:
       i. Internet browsing
       ii. Email
       iii. Any other non-PCS access to remote systems or services
    b. Implement mobile device and portable media controls.

12. **Cyber Informed Engineering**
    a. Conduct a consequence / impact analysis to prioritize scenarios.
    b. Design and implement a system architecture to limit the potential impacts of an attack.
    c. Include engineered controls in addition to traditional IT controls.
    d. Simplify system design to the extent practical.
    e. Conduct resilience planning to improve response and recovery actions.
    f. Control information on the engineering of the system to prevent unwanted distribution.
    g. Control procurement processes.

h. Control system interdependencies.

i. Establish and maintain a cyber-aware culture of employees, contractors, and visitors.

j. Complete a digital asset inventory to document hardware, software, and firmware currently in use.

13. Education

a. Implement a cybersecurity awareness program that includes social engineering.

b. Provide on-going cross training for enterprise system and PCS staff that identifies current best practices and standards for PCS cybersecurity.

c. Provide basic network and radio communications training for PCS technicians.

d. Participate in water sector programs that facilitate cybersecurity knowledge transfer.

e. Identify appropriate certifications for internal and external staff. Include certification requirements in SLAs and contracts with external service providers.

f. Provide periodic security awareness training to all employees that identifies risky behaviors and threats.

g. Promote information sharing within your organization.

14. Personnel Security

a. Implement a personnel security program for internal and contracted personnel that includes:

   i. Training

   ii. Periodic background checks

b. Require annual and new employee signoff on cybersecurity policy(ies), which includes agreeing to a confidentiality statement

AWWA Assessment Tool Output

The AWWA Assessment Tool currently produces an automatically generated output file to help utilities achieve both compliance and improve their cybersecurity posture. This file is designed to facilitate a cycle of improvement through an easily repeatable and documentable process. These outputs are detailed in the following sections.

This output is automatically generated as a Microsoft Excel spreadsheet workbook. This file is designed to support utilities with compliance requirements of AWIA §2013. In addition, the output file is formatted in a manner to support building an improvement plan. Use of this output file involves the following steps:

➢ Step 1. Select the implementation status of each recommended control from a drop-down list on the RRA-Control tab.

➢ Step 2. Review the results on the RRA-Control Status Summary tab.

➢ Step 3. On the ERP-Improvement Projects tab, select the table column headers, navigate to the Data tab at the top of the spreadsheet, and select the Filter tool in your Excel ribbon. On the Improvement Project column, click the filter icon in the cell and select "Partially Implemented" and "Planned and Not Implemented." On the Priority column select "Sort Smallest to Largest." Sorting by Control Status and Priority allows the user to identify the highest priority

recommended controls for implementation. Additional grouping of the recommended controls may be done by sorting of the "Improvement Projects" column.

➢ Step 4. Use the project implementation plan to design cybersecurity improvement projects.

➢ Step 5. Complete the Declaration of Due Diligence for communication with utility leadership and for documenting compliance.

➢ Step 6. Print the results for inclusion with compliance documentation, communication with stakeholders, and improvement project/risk and resilience management strategy development.

There are seven tabs in the file, including:

Tab 1. **Start Here** – This tab provides context and high-level instructions for the use of the output file.

Tab 2. **RRA-Control Output** – This summarizes the recommended cybersecurity controls, provides users the functionality to document the recommenced cybersecurity control status, and identifies improvement projects. This tab is designed to facilitate compliance with the RRA requirements included in AWIA §2013. This is the only tab that requires user input.

Tab 3. **RRA – Control Status Summary** – This tab provides two tables. The first summarizes the recommended controls' status by priority. This is shown in a "heat map" format to visually indicate the number of controls of various priority and their associated status. The second table identifies the number of controls associated with each improvement project categories as identified in the guidance document. These projects account for recommended controls where the user indicated "Partially Implemented" or "Planned and Not Implemented" on the RRA-Control Output tab.

Tab 4. **ERP-Improvement Projects** – This tab provides two tables. The first is the same as the second table on tab 3. The second table is a sorted version of the controls summarized on tab 2. The intent of this second table is to allow the user to aggregate controls into projects. This table provides Priority 1 controls across each practice area. This tab is designed to facilitate compliance with the ERP requirements included in AWIA §2013. Mitigation strategies and resources may include equipment, policies and people. Once controls are aggregated into projects on this sheet, these may be grouped together using the Project Implementation Form included as tab 5.

Tab 5. **Project Implementation Form** – This is an optional sample project planning form. Full completion of the information in this form will facilitate successful project delivery.

Tab 6. **Declaration of Due Diligence** – The optional draft form is provided for use with the AWWA Assessment Tool output. The draft text is intended to facilitate communication with utility decision makers and support long-term cybersecurity risk management.

Tab 7. **User Answer Summary** – This tab provides a summary of AWWA Assessment Tool questions and associated user answers. Also included on this tab is a control status summary table. This table is presented in a "heat map" format to visually indicate the importance of controls by priority and status.

Additional details for the RRA-Control Output (Tab 3) and ERP-Improvement projects tabs (Tab 4) are provided in the following sections.

RRA-Control Output Tab

The RRA-Control Output tab is designed to facilitate compliance with the RRA requirements included in AWIA §2013 by supporting "…assessment of the risks to, and resilience of, its system." This tab lists each of the controls recommended by the tool based on the user inputs. The recommended controls are categorized into Priorities 1, 2, 3, and 4, with Priority 1 being the highest. For each control, there are multiple columns that are available to the user to provide documentation of the level of implementation of each control at their organization.

Within this tab, the Control Status column is the only column that requires additional user input. The cells requiring input are colored blue for identification purposes. The user must select the implementation status of the recommended control within the utility/system/facility under evaluation.

The options for implementation levels include:

1. **Not Planned and/or Not Implemented** – Risk Accepted – The control is not currently implemented or planned for implementation. The organization accepts risks associated with the control not being implemented.
2. **Planned and Not Implemented** – The control has not been implemented. However, implementation of the control is planned.
3. **Partially Implemented** – The control is partially implemented by internal or external resources.
4. **Fully Implemented and Maintained** – The control is fully implemented and actively maintained by internal or external resources.

Utility staff should use the output to document controls already in place and those that are most important to implement. This will likely require working with additional stakeholders to document the state of implementation of the various recommended controls. Improvement project categories are provided for each recommended control.

ERP-Improvement Projects Tab (Tab 4)
This tab is designed to facilitate compliance with the ERP requirements included in AWIA §2013 (b) "Emergency Response Plan", including:

- "(1) strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;"
- "(2) plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water;"
- "(3) actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers; and"
- "(4) strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system."

There are two tables within this output tab. The first is the Cyber Resilience Improvement Projects table. This table identifies improvement projects and the associated number of controls. Additional rows are available for user-identified projects. These projects address all recommended controls where the user indicated "Partially Implemented" or "Planned and Not Implemented."

The second table is the Control Summary. This table provides a summary of controls and levels of implementation from user input on the RRA-Control Output tab. This is provided in a heat map format to allow a utility to easily see a high-level control summary organized by control status and priority.

Utility staff should use this output to create an implementation strategy for the most important controls identified by the RRA Support Output. It is important to note that this will likely require working with additional stakeholders to document a strategy for implementation of additional controls.

REFERENCE STANDARDS

To provide the user with more detailed information on the steps necessary to implement the recommended cybersecurity controls, specific references to existing AWWA, NIST, and International Society of Automation (ISA) standards are provided. The references provide the specific paragraph or section number in the referenced standard in which the applicable information can be found. Table 3 provides a list of the referenced standards. Each standard listed is publicly available; however, access to several of the standards listed below require payment.

List of Standards & Guidance

	Name	Version/Revision Date
ANSI/AWWA G430-14	Security Practices for Operation and Management	November 2014
ANSI/AWWA G440-17	Emergency Preparedness Practices	August 2017
AWWA J100-10 (R13)	Risk and Resilience Management of Water and Wastewater Systems	2013
AWWA Manual M19	Emergency Planning for Water and Wastewater Utilities, Fifth Edition	2018
DHS-CAT	U.S. Department of Homeland Security (DHS) Catalog of Control Systems Security: Recommendations for Standards Developers	April 2011
DHS ICS-CERT	Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies	September 2016
HIPAA	45 Code of Federal Regulations (CFR) Part 160 and Part 164	August 2002
INL CIE	Cyber-Informed Engineering	March 2017
ISA 62443-1-1	Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models	October 2007
ISA 62443-2-1	Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program	January 2009
ISA TR62443-2-3-2015	Security for industrial automation and control systems Part 2-3: Patch management in the IACS environment	2015
ISA 62443-3-3	Security for industrial automation and control systems	August 2013

	Name	Version/Revision Date
	Part 3-3: System security requirements and security levels	
ISA-62443-4-1-2018	ANSI/ISA-62443-4-1-2018, Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements	2018
ISA-62443-4-2-2018	Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components	2018
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements	October 2013
ISO/IEC 27003	Information technology — Security techniques — Information security management system implementation guidance	February 2010
ISO/IEC 27005	Information technology — Security techniques — Information security risk management	June 2011
PCI-DSS v3.2.1	Payment Card Industry – Data Security Standard	May 2018
NIST Cybersecurity Framework	Cybersecurity Framework v1.1	April 2018
NIST 800-34r1	Contingency Planning Guide for Federal Information Systems	May 2010
NIST 800-53r4	Security and Privacy Controls for Federal Information Systems and Organizations	April 2013
NIST 800-61r2	Computer Security Incident Handling Guide	August 2012
NIST 800-82r2	Guide to Industrial Control Systems (ICS) Security	May 2015
NIST 800-124r1	Guidelines for Managing the Security of Mobile Devices in the Enterprise	June 2013
NIST 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	April 2015
Various	State specific data breach laws	Various

Appendix A: America's Water Infrastructure Act (AWIA) of 2018 §2013

SEC. 2013. COMMUNITY WATER SYSTEM RISK AND RESILIENCE.

(a) Risk and Resilience Assessments.-

(1) In general.-- Each community water system serving a population of greater than 3,300 persons shall conduct an assessment of the risks to, and resilience of, its system. Such an assessment—

(A) shall include an assessment of—

(i) the risk to the system from malevolent acts and natural hazards;

(ii) the resilience of the pipes and constructed conveyances, physical barriers, source water, water collection and intake, pretreatment, treatment, storage and distribution facilities, electronic, computer, or other automated systems (including the security of such systems) which are utilized by the system;

(iii) the monitoring practices of the system;

(iv) the financial infrastructure of the system;

(v) the use, storage, or handling of various chemicals by the system; and

(vi) the operation and maintenance of the system; and

(B) may include an evaluation of capital and operational needs for risk and resilience management or the system.

(2) Baseline information.--The Administrator, not later than August 1, 2019, after consultation with appropriate departments and agencies of the Federal Government and with State and local governments, shall provide baseline information on malevolent acts of relevance to community water systems, which shall include consideration of acts that may--

(A) substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; or

(B) otherwise present significant public health or economic concerns to the community served by the system.

(3) Certification.—

(A) Certification.--Each community water system described in paragraph (1) shall submit to the Administrator a certification that the system has conducted an assessment complying with paragraph (1). Such certification shall be made prior to—

(i) March 31, 2020, in the case of systems serving a population of 100,000 or more;

(ii) December 31, 2020, in the case of systems serving a population of 50,000 or more but less than 100,000; and

(iii) June 30, 2021, in the case of systems serving a population greater than 3,300 but less than 50,000.

(B) Review and revision.--Each community water system described in paragraph (1) shall review the assessment of such system conducted under such paragraph at least once every 5 years after the applicable deadline for submission of its certification under subparagraph (A) to determine whether such assessment should be revised. Upon completion of such a review, the community water system shall submit to the Administrator a certification that the system has reviewed its assessment and, if applicable, revised such assessment.

(4) Contents of certifications.--A certification required under paragraph (3) shall contain only--

    (A) information that identifies the community water system submitting the certification;

    (B) the date of the certification; and

    (C) a statement that the community water system has conducted, reviewed, or revised the assessment, as applicable.

(5) Provision to other entities.--No community water system shall be required under State or local law to provide an assessment described in this section (or revision thereof) to any State, regional, or local governmental entity solely by reason of the requirement set forth in paragraph (3) that the system submit a certification to the Administrator.

(b) Emergency Response Plan.--Each community water system serving a population greater than 3,300 shall prepare or revise, where necessary, an emergency response plan that incorporates findings of the assessment conducted under subsection (a) for such system (and any revisions thereto). Each community water system shall certify to the Administrator, as soon as reasonably possible after the date of enactment of America's Water Infrastructure Act of 2018, but not later than 6 months after completion of the assessment under subsection (a), that the system has completed such plan. The emergency response plan shall include—

(1) strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system;

(2) plans and procedures that can be implemented, and identification of equipment that can be utilized, in the event of a malevolent act or natural hazard that threatens the ability of the community water system to deliver safe drinking water;

(3) actions, procedures, and equipment which can obviate or significantly lessen the impact of a malevolent act or natural hazard on the public health and the safety and supply of drinking water provided to communities and individuals, including the development of alternative source water options, relocation of water intakes, and construction of flood protection barriers; and

(4) strategies that can be used to aid in the detection of malevolent acts or natural hazards that threaten the security or resilience of the system.

Appendix B: Network Architecture Reference Diagram and Definitions

PCS and enterprise system architecture provides an extensive list of new terminology for users of this guidance document and AWWA Assessment Tool to learn and understand. The Industrial Control System – Computer Emergency Response Team (ICS-CERT) has provided an exceptional resource for PCS owners and operators to refer to. The secure architecture design in Figure 3 [12] "is the result of an evolutionary process of technology advancement and increasing cyber vulnerability presented in the Recommended Practice document, *Control Systems Defense in Depth Strategies*." [13] While this is specifically directed at PCS owners and operators, much of the terminology is compatible with enterprise systems.

---

[12] ICS-CERT. *Secure Architecture Design*. https://ics-cert.us-cert.gov/Secure-Architecture-Design#nogo. Last accessed May 1, 2019

[13] DHS. *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf. Last accessed May 1, 2019. September 2016.
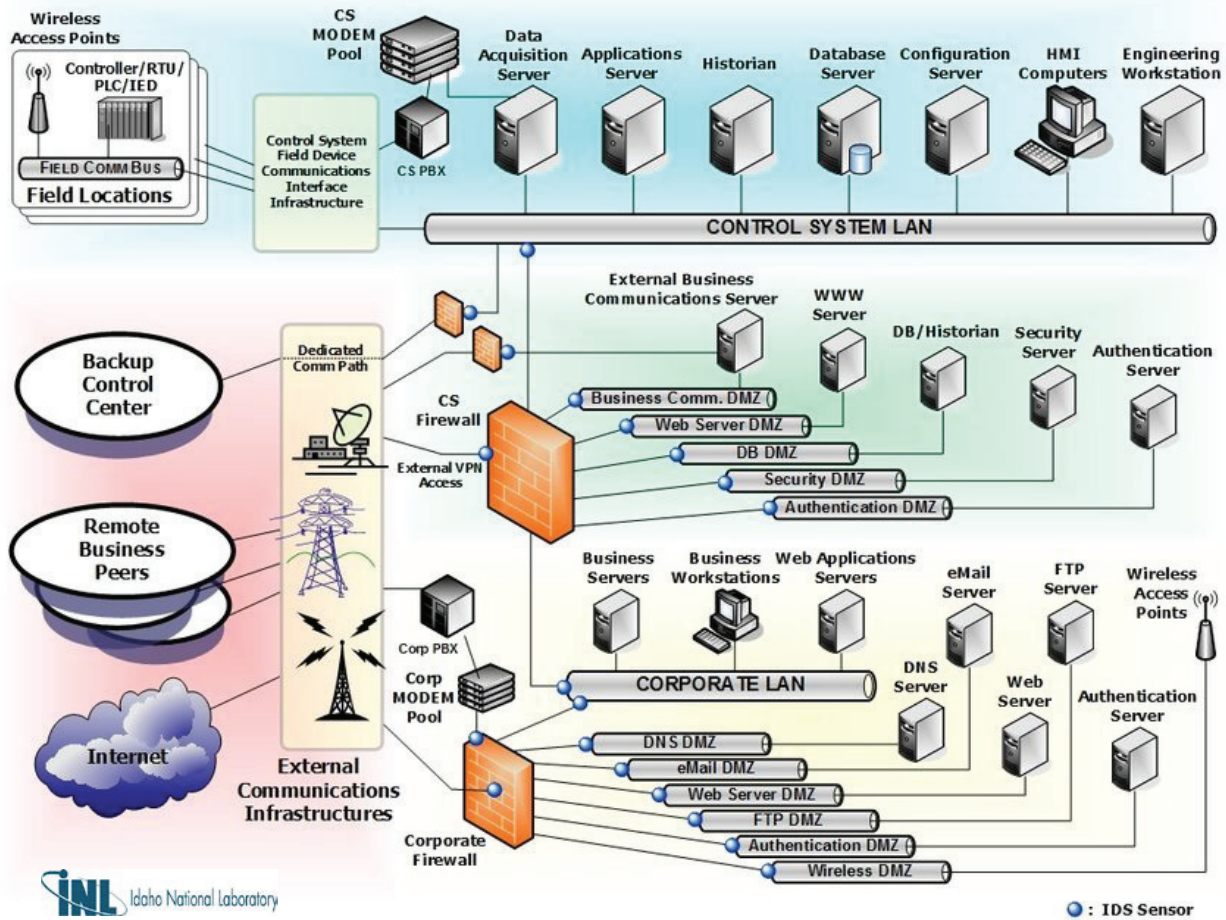
Figure 3. Secure Architecture Design

Appendix C: User Interface Questions

#	Question	Additional Details	Yes /No
1	Are any data transferred to or from your PCS network, by any electronic means?	Examples of electronic data transfer include both automatic (e.g. automated export of data from the PCS environment) and manual (e.g. transfer of data to/from the PCS environment via thumb drive). Examples of data that may be transferred include: • Water quality data collected by the PCS and transferred for regulatory reporting • Asset performance data for asset management • Operating system / software patches and updates	
2	Do users manually transfer any electronic data to or from your PCS environment?	Users include anyone internal or external with access to PCS. This may include operators, technicians, and third-party consultants. Users are able to initiate transfer of data to and from the PCS. Examples of manual data transfer include: • USB • Portable media device • Temporary network connections (an ad hoc network connection for transferring data from one computer to another) • Shared drives • Cloud file share (e.g. DropBox)	
3	Are any electronic data transferred to or from your PCS environment using an automated process, without user interaction?	Examples of automated transfer of data include: • Automated software or firmware updates • Licensing • Operating System updates • Antivirus signatures • Database transfer • Network monitoring by devices external to the PCS	

#	Question	Additional Details	Yes /No
4	Are any users allowed to access your PCS environment remotely?	Users include any personnel with internal or external access to the PCS environment. These may include operators, technicians, and third-party consultants. Devices can be any network enabled device either corporate supplied or personal. Examples of remote access include: • Operations staff access the PCS environment from mobile device. This includes web view and read only. • Users have access to remote physical site using any non-PCS environment.	
5	Is remote access to your PCS network allowed via mobile devices?	Devices can be any network enabled device either corporate supplied or personal. This includes web view and read only. Examples of mobile devices include: • Laptops • Tablets • Cellphones • Smart Phones	
6	Is remote access to your PCS allowed at physically secured fixed location(s)?	Examples of remote access from physically secured fixed location include: • Control center managing remote sites • Control center remotely managing a treatment center • Office desktop computer • Computer at secured office used for managing remote booster station	
7	Do you use resources outside your organization to support and/or maintain your PCS environment?	Examples of resources outside of the organization supporting and/or maintaining your PCS environment include: • Subsystems owned and operated by 3rd party • Systems Integrators • Equipment Manufacturers • Consultants • Vendors	

#	Question	Additional Details	Yes/No
8	Do resources (e.g. service providers) outside your organization provide PCS support via remote access?	Examples of resources outside your organization providing support by remote access includes: • "Black box" solution vendor - "Black box" refers to piece of equipment on a network with contents and/or function that are unknown to the user/owner/operator. • Vendor panel solution - Vendor panel refers to a control panel provided by a vendor to monitor or operate a treatment or distribution process. For example: a vendor provided ultrafiltration unit would have an accompanying control panel to control the ultrafiltration process. • Network administration, from external sources.	
9	Do internal staff provide support for your PCS via remote access?	Remote access is from outside (for example, from home) of the controlled or control room environments. Devices can be any smart phone, tablet, laptop either corporate supplied or personal. Examples of internal staff providing support by remote access include: • Remote operation and monitoring • Remote troubleshooting	
10	Are all changes or updates made to your PCS environment first tested in a development, testbed, non-production, and/or training environment prior to being deployed and implemented in the field/production environment?	• These changes/updates include any programming of logic controllers, human machine interfaces, instrumentation, or any devices involved with the PCS. • System changes or updates do not negatively impact PCS operation. • PCS changes are tested in a non-production environment before they are made in the field/production environment. • Testing is performed to ensure the proper operation and interaction with other system components before deployment. • Changes or updates may be made by either internal or external resources.	
11	Does your PCS include 3rd party network communication services?	Examples of 3rd party network communications services include: • Cellular (3G, 4G, 5G) • Dedicated leased line (copper, fiber) • Communication over internet • City/county communication network not dedicated to PCS	

#	Question	Additional Details	Yes /No
12	Does your PCS network use licensed or unlicensed wireless radios between facilities?	Unlicensed wireless spectrum frequencies – Unlicensed wireless devices operate in one of the frequency bands set aside by the Federal communications Commission (FCC) for industrial, scientific or medical (ISM) applications. Frequencies within the unlicensed wireless spectrum are free to use. Licensed wireless spectrum frequencies – Frequencies or frequency bands designated by the Federal Communications Commission (FCC) as reserved for organizations with licenses. Examples of licensed or unlicensed wireless spectrum services include: • Radio - 450MHz • Radio - 900MHz • WiFi - 2.4GHz • WiFi - 5GHz • WiFi - 6GHz • Microwave	
13	Does your PCS share a LAN or WAN with non-PCS equipment?	Examples of non-PCS equipment include: • Security cameras • Access control equipment • Enterprise network services at a facility with a shared communication path • Voice over Internet Protocol (VOIP) • Fire Alarms • Vault or Panel Intrusion Alarms	
14	Do you use Wi-Fi within the PCS environment to transfer data in support of operations or monitoring?	• Does your PCS communication network have wireless access points? • Wi-Fi is defined in IEEE 802.11	
15	Do you use virtualization technology for your PCS?	Virtualization Technology – Technology capable of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources. Examples of virtualization technology include: • VMware • Oracle VM • HyperV	

#	Question	Additional Details	Yes /No
16	Is the virtualization technology dedicated to PCS only?	Virtualization Technology – Technology capable of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources. • A separate physical host(s) is used for PCS virtual machines. • All non-PCS virtual machines reside on non-PCS physical host(s).	
17	Does your organization accept, process, store or transmit credit card or debit card information, or accept payment with pre-paid cards branded with American Express, Discover, JCB, MasterCard or Visa International logos?	This information may be collected and stored for service payment purposes. Using a third-party company for processing PCI may cut down on risk exposure but does not exclude a company from PCI DSS compliance. Customer billing information including: • Credit/debit card numbers • Credit/debit card numbers with name, expiration date or service code • Sensitive authentication data (including magnetic stripe, PINs, CVV, etc.) NOTE: Includes organizations that have outsourced payment services.	
18	Does your organization own, license, acquire or maintain any personally identifiable information (PII)?	PII is any information that may be used to identify an individual. This includes customers, employees, and contractors. Examples of PII include: • Customer billing information and addresses • Employee personal information, including SSN, birthdate, etc. Each state has its own data breach notification law(s) regarding PII. Depending on the state statute, a non-exhaustive list of possible examples may include (alone or in conjunction with other information) tax identification numbers, social security numbers, government issued identification numbers, account numbers, health information, email addresses in conjunction with a password, unique biometric information, etc.	

#	Question	Additional Details	Yes /No
19	Is your organization an employer that creates or receives health information that is HIPAA protected?	HIPAA defines protected health information (written, electronic, or oral) as information, including demographic data, that identifies an individual (or there is a reasonable basis to believe it can identify an individual) and that relates to: • the individual's past, present or future physical or mental health or condition, • the provision of health care to the individual, or • the past, present, or future payment for the provision of health care to the individual. Examples of HIPAA protected information include: • Employee medical records • Employee vaccine records • Health and safety records may include HIPAA protected records • Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).	
20	Is your organization responsible for the engineering design and implementation of critical infrastructure?	The water/wastewater sector is defined as critical infrastructure by the federal government (42 U.S.C. 5195(e)). Examples of holding responsibility for engineering services include: • Utility has an internal engineering department • Utility hires engineering consultants • You are part of a stakeholder organization that has internal resources or hires external resources to design and implement critical infrastructure	
21	Does your organization have a supply chain risk management program?	Do you currently require your supplier to provide any chain-of-custody documents? An example of supply chain risk management program includes ordering and confirming treatment chemicals are NSF certified.	

#	Question	Additional Details	Yes /No
22	Does your organization have a supply chain risk management program that specifically addresses cybersecurity?	Does the supply chain risk management program specify how delivery for procured products – hardware, software, and/or data will be validated and monitored to ensure their integrity? Examples of specifically addressing cybersecurity in supply chain risk management include: • Documenting information protection practices of supplier • Integrity management program for components provided by sub-suppliers • Supplier contracts include appropriate language to meet objectives of the organization's cybersecurity program	

Appendix D: Cybersecurity Use-Cases

Category/ Code	Use Case	Description
Architecture		
AR1	Dedicated Process Control Network	All network and communications infrastructure is dedicated exclusively to SCADA with no equipment or communications paths shared with non-SCADA networks.
AR2	Shared WAN	Network wide-area communications infrastructure is shared with some non-SCADA networks.
AR3	Shared LAN	Network local-area communications (within control system) is shared with non-SCADA networks.
AR4	Unlicensed wireless Wide-Area (site-to-site) Network	Network wide-area communications fully or partially comprised of wireless links using unlicensed (ISM 900 MHz, 2.4 or 5 GHz) spectrum.
AR5	Licensed wireless Wide-Area (site-to-site) Network	Network wide-area communications fully or partially comprised of wireless links using licensed spectrum.
AR6	Communications via Internet	Network wide-area communications fully or partially comprised of links over Internet services using public address space.
AR7	Communications via 3rd party carrier	Network wide-area communications fully or partially comprised of links over 3rd party carrier services (e.g. cellular, Metro-E/Ethernet/LAN).
AR8	Dedicated process control server virtualization	Virtualized server infrastructure dedicated to SCADA/Process Control with no equipment shared with non-SCADA/Process Control systems.
AR9	Shared server virtualization	Virtualized server infrastructure shared between SCADA/Process Control and non-SCADA/Process Control systems.
AR10	802.11 Wireless used in Control System	802.11 unlicensed wireless technologies used within control system.
AR11	Connection to non-SCADA Network	Connection to non-SCADA network through direct connection or firewall/DMZ.
Network Management & System Support		
NM1	Local network management and system support by SCADA/Process Control personnel in physical proximity of equipment	Access to configure network infrastructure located in immediate vicinity of user (serial or network) by SCADA/Process Control personnel.
NM2	Plant network management and	Access to configure network equipment located on same facility from centralized location by SCADA/Process Control personnel.

Category/Code	Use Case	Description
	system support by SCADA/Process Control personnel	
NM3	Remote network management and system support by SCADA/Process Control personnel	Access to configure network infrastructure located in another physical facility by SCADA/Process Control personnel.
NM4	Local network management and system support by non-SCADA/Process Control personnel	Access to configure network equipment located in immediate vicinity of user (serial or network) by non-SCADA/Process Control personnel.
NM5	Plant network management and system support by non-SCADA/Process Control personnel	Access to configure network equipment located in another physical facility by non-SCADA/Process Control personnel.
NM6	Remote network management and system support by non-SCADA/Process Control personnel	Access to configure network infrastructure located in another physical facility by non-SCADA/Process Control personnel.
Program Access		
PA1	Outbound messaging	Automated, non-interactive sending of SMTP, SMS or other outbound alarms and messaging from system.
PA2	Outbound file transfer	Interactive sending of files from system to other locations by user.
PA3	Inbound file transfer	Interactive receiving of files from other locations to system by user.
PA4	Software updates	Automated, non-interactive retrieval of licensing, OS updates, anti-virus signatures and other system data from other locations to system.
PA5	Data exchange	Automated, non-interactive exchange of data (e.g. database-to-database exchange, ntp or other external data) with systems located externally. (Implies full-time connection.)
PA6	Network management communications	Automated, non-interactive exchange of network management data (e.g. syslog, SNMP traps, SNMP polling) with system(s) located external to system. (Implies full-time connection.)

Category/ Code	Use Case	Description
PLC Programming and Maintenance		
PLC1	Local PLC programming and maintenance	Access to PLC programming and maintenance is local to device (serial or network).
PLC2	Plant PLC programming and maintenance	Access to PLC programming and maintenance from a centralized on-site location.
PLC3	Remote PLC programming and maintenance	Access to PLC programming and maintenance from an off-site location.
PLC4	Third party SCADA/Process Control presence	SCADA/PCS equipment (e.g. PLC, RTU) owned and operated by third party (e.g. business partner) located on SCADA/Process Control network with external access by third party.
PLC5	Third party SCADA/Process Control package systems	SCADA/PCS sub-systems owned and operated by third parties located within plant facility with direct network connection to SCADA/Process Control system (package system) with on-site access by third party.
User Access		
UA1	Control room system access with control	Access to system with full read-write capability from on-plant, physically-secure "control room" location.
UA2	Plant system access with control from fixed locations	Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor).
UA3	Remote system access with control from fixed locations	Access to system with full read-write and/or read-only/view-only capability from location outside "control room" environment and located outside the physical perimeter of the facility workstations or HMI.
UA4	Remote system access with web view from fixed locations	Access to web displays of system data with read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility via web browser on non-dedicated computer.
UA5	Plant system access with control from mobile device	Access to system with full read-write capability from on-plant location, not physically secured (e.g. plant floor) on mobile device.
UA6	Remote system access with control from mobile device	Access to system with full read-write capability from location outside "control room" environment and located outside the physical perimeter of the facility on mobile device.
UA7	Remote system access with	Access to system with limited read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility on mobile device.

Category/ Code	Use Case	Description
	view-only from mobile device	
UA8	Remote system access with web view from mobile device	Access to web displays of system data with read-only/view capability from location outside "control room" environment and located outside the physical perimeter of the facility via web browser on non-dedicated mobile device.
UA9	Training environment	System training conducted on production SCADA/Process Control system by third parties.
UA10	Development environment by SCADA/Process Control staff	System development conducted on production SCADA/Process Control network by SCADA/Process Control personnel.
UA11	Development environment by external staff or third parties	System development conducted on production SCADA/Process Control network by non-SCADA/Process Control personnel.
Data Security		
DS1	Accept, store or process credit card information	Organization accepts, processes, stores, or transmits credit or debit card information or certain pre-paid payment cards.
DS2	Storage of PII	Organization owns, licenses, acquires or maintains PII.
DS3	Storage or maintenance of protected health information that is HIPAA protected.	Organization creates or receives protected health information.
Cyber Informed Engineering		
CIE1	Engineering design and implementation of critical infrastructure.	A program is in place to engage engineering staff in understanding and mitigating high-consequence and constantly evolving cyber threat during the design and implementation phase.
Supply Chain		
SU1	Supply chain risk management program	Organization has a supply chain risk management program.
SU2	Supply chain risk management program cybersecurity.	Organization's supply chain risk management process addresses cybersecurity.

Appendix E: Cybersecurity Controls

AT: Awareness and Training		Cybersecurity Practice Areas/Recommended Projects	Additional Details
AT-1	A general security awareness and response program established to ensure staff is aware of the indications of a potential incident, security policies, and incident response/notification procedures.	Education	An operator finds a USB media device. Based on their cybersecurity training, they know not to use it on the company network.
AT-2	Job-specific security training including incident response training for employees, contractors and third-party users.	Education; Cyber-Informed Engineering	An operator has received what they believe to be a malicious email. They recognize that it is a phishing attack based on security training awareness programs the company has in place.
AT-3	A forensic program established to ensure that evidence is collected/handled in accordance with pertinent laws in case of an incident requiring civil or criminal action.	Governance and Risk Management	A SCADA tech believes a machine is infected. Based on their training, they remove the machine from the network and report it to Information Technology Team (IT) without powering it off to avoid deleting evidence.
AU: Audit and Accountability		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
AU-1	Audit program established to ensure information systems are compliant with policies and standards and to minimize disruption of operations.	Application Security; Governance and Risk Management	IT schedules an independent review and examination of records and activities to assess the adequacy of system controls and to ensure compliance with established policies.
AU-2	Framework of information security policies, procedures, and controls including management's initial and periodic approval established to provide governance, exercise periodic review, dissemination, and coordination of information security activities.	Governance and Risk Management	A third-party system integrator asks the SCADA tech to email a document with sensitive network information. The SCADA tech refuses and notifies integrator of the secure file transfer system in place.
AU-3	Governance framework to disseminate/decentralize decision making while maintaining executive authority and strategic control and ensure that managers follow the security policies and enforce the execution of security procedures within their area of responsibility.	Governance and Risk Management	Data security policy and controls are in place to prevent sharing of private or sensitive data outside of the organization.
AU-4	Information security responsibilities defined and assigned.	Governance and Risk Management	All staff are aware of who they would report to if they notice suspicious behavior in the system.

AU-5	Risk based business continuity framework established under the auspices of the executive team to maintain continuity of operations and consistency of policies and plans throughout the organization. Another purpose of the framework is to ensure consistency across plans in terms of priorities, contact data, testing, and maintenance.	Business Continuity and Disaster Recovery	The facility has a documented and tested contingency plan to operate the facility without the use of SCADA software, in the case of attack by ransomware.
AU-6	Policies and procedures established to validate, test, update and audit the business continuity plan throughout the organization.	Governance and Risk Management; Business Continuity and Disaster Recovery	The business continuity plan is revised annually. Revisions are informed by planned exercises, actual events, or documented changes.
AU-7	Policies and procedures for system instantiation/deployment established to ensure business continuity.	Business Continuity and Disaster Recovery	The PCS has a testing/development environment to allow changes to be implemented without immediate effects to the production environment.
AU-8	Template for the organization's confidentiality/non-disclosure agreements defined, reviewed, and approved periodically by management.	Governance and Risk Management	Reviews of the organization's confidentiality/non-disclosure agreements are periodically scheduled by a responsible party.
CM: Configuration Management		**Cybersecurity Practice Areas/ Recommended Projects**	**Additional Details**
CM-1	Policies for defining business requirements including data validation and message authenticity established to ensure that new/upgraded systems contain appropriate security requirements and controls.	Governance and Risk Management	Meetings are periodically scheduled between management and IT to discuss current and potential cybersecurity risks and the impact on business decisions.
CM-2	Procedure modification tracking program in place to manage and log changes to policies and procedures.	Governance and Risk Management	The Emergency Response Plan is stored in a central repository and clearly displays the version and date of when it was implemented.
CM-3	Separation of duties implemented for user processes including risk of abuse.	Application Security; Governance and Risk Management	Operators are only given clearance to areas they are expected to work in. Supervisors have the ability and training to monitor SCADA tech activities in the PCS.
CM-4	Separation of duties implemented for development, production, and testing work.	Application Security; Personnel Security; Governance and Risk Management	A SCADA technician must have a second technician review changes made to production equipment before they are implemented.
CM-5	SLAs for all third parties established, including levels of service and change controls.	SLA	A security policy that outlines which access permissions are distributed to third party employees.
CM-6	Risk based policies and procedures for change controls, reviews, and audits of SLAs.	Governance and Risk Management	Inviting all affected parties to discussions to prevent the development of vulnerabilities in the facility.
CM-7	Monitoring of resources and capabilities with notifications and alarms established to alert management when resources/capabilities fall below a threshold.	Telecommunications, Network Security, and Architecture; SLA	IT monitors SCADA computers for processor usage that could indicate cryptojacking activity.

A: Identification and Authentication & Access Control		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
IA-1	Access control policies and procedures established including unique user ID for every user, appropriate passwords, privilege accounts, authentication, and management oversight.	Access Control; Application Security; Governance and Risk Management	Based on their knowledge of access control policies, operators do not share passwords.
IA-2	Access control for the management, monitoring, review, and audit of accounts established including access control, account roles, privilege accounts, password policies and executive oversight.	Access Control; Application Security; Governance and Risk Management	Upon staff termination or resignation, login credentials are disabled as part of the Human Resources process.
IA-3	Role based access control system established including policies and procedures.	Access Control; Application Security; Governance and Risk Management	SCADA software implements unique usernames and passwords with different levels of control based on roles.
IA-4	Access control for confidential system documentation established to prevent unauthorized access of trade secrets, program source code, documentation, and passwords (including approved policies and procedures).	Access Control; Application Security; Governance and Risk Management	A third-party system integrator asks the SCADA tech to email a document with sensitive network information. The SCADA tech refuses and notifies integrator of the secure file transfer system in place.
IA-5	Access control for diagnostic tools and resources and configuration ports.	Access Control	PLC programming software is only available at select workstations and only accessible to SCADA technicians.
IA-6	Access control for networks shared with other parties in accordance with contracts, SLAs and internal policies.	Access Control; Service Level Agreements; Governance and Risk Management	Contracts with third-party equipment vendors establish security requirements for remote access to equipment.
IA-7	Wireless and guest-access framework established for the management, monitoring, review, and audit of wireless and guest access in place.	Access Control; Governance and Risk Management	To use the plant guest network, users are required to accept a user agreement.
IA-8	Policies for security of standalone, lost, and misplaced equipment in place.	Governance and Risk Management	An operator misplaces a managed phone. Based on the missing equipment policy, they contact IT to report the device lost.
IA-9	Multifactor authentication system established for critical areas.	Access Control	Remote access to the SCADA system requires two factor-authentication.
IA-10	Policies and procedures for least privilege established to ensure that users only gain access to the authorized services.	Governance and Risk Management	Idle sessions on SCADA screens are logged off in 15 minutes. If no user is logged in, a read-only view is presented.
IA-11	Workstation and other equipment authentication framework established to secure sensitive access from certain high-risk locations.	Access Control	The controls to critical equipment are only available at a local secured terminal.
IA-12	Session controls established to inactivate idle sessions, provide web content filtering, prevent access to malware sites, etc.	Access Control	An operator attempts to connect to a known hacking website. The connection is blocked. The operator and IT are notified of the attempt.

IR: Incident Response, Contingency Planning, & Planning		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
IR-1	Incident response program established with a formal Emergency Response Plan to restore systems and operations based on their criticality and within time constraints and effect recovery in case of a catalogue of disruptive events. Exercises conducted to test and revise plans and build organizational response capabilities.	Governance and Risk Management; Data Security	Emergency Response Plan includes procedures for recovering SCADA system operation from system backup.
IR-2	A security program established with a formal Emergency Response Plan to respond to security incidents monitor, discover, and handle security alerts and technical vulnerabilities, collect and analyze security data, limit the organization's risk profile and ensure that management is aware of changing/emerging risks.	Governance and Risk Management; Data Security	A SCADA tech believes a machine is infected and responds according to the utility's emergency response plan for cybersecurity based incidents.
IR-3	A legal/contractual/regulatory framework established with a formal Emergency Response Plan to track legal/contractual/regulatory requirements and the efforts to meet them with respect to each important system within the organization. Another purpose of the framework is to ensure compliance of policies and procedures with privacy laws, handling cryptographic products, intellectual property rights, and data retention requirements.	Governance and Risk Management; Data Security	The Emergency Response Plan is reviewed and updated once a year by responsible staff.
MA: Maintenance		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
MA-1	Equipment maintenance/replacement program established to maintain business continuity, availability, and integrity.	Service Level Agreement Governance and Risk Management; Cyber-Informed Engineering	Based on the company's controlled maintenance program, a utility will format network devices to factory settings before sending them out of the organization for maintenance.
MA-2	Maintenance of relationships with authorities, professional associations, interest groups etc., formalized. This is done, in part, to maintain an up-to-date situational awareness of relevant threats.	Governance and Risk Management	The utility is a member of DHS's ICS-CERT mailing list to receive frequent communications on PCS vulnerabilities discovered and patches available. SCADA techs regularly review alerts to determine if the alerts are applicable to their system.
MA-3	Off-site equipment maintenance program including risk assessment of outside environmental conditions established.	Governance and Risk Management	The condition of offsite equipment and risk factors acting on the equipment are periodically reviewed and assessed via an independent party.

MP: Media Protection		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
MP-1	Storage media management and disposal program established to ensure that any sensitive data/software is used appropriately and is removed prior to media disposal (including approved policies and procedures).	Governance and Risk Management	When decommissioning a network device that was used in the production environment, IT is required to return it to factory conditions before it leaves the facility.
MP-2	Information exit mechanisms in place to prevent data, software leaving premises without authorization or logging.	Governance and Risk Management	The Emergency Response Plan is stored in a central repository that records when files are accessed and altered.
MP-3	Policies and procedure repository in place to be available to all authorized staff.	Governance and Risk Management	Company policies and procedures are available in a central, secure, shared location.

PE: Physical and Environmental Protection		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
PE-1	Security perimeters, card-controlled gates, manned booths, and procedures for entry control.	Access Control; Physical Security	Personnel are required to present a badge to access the PCS.
PE-2	Secure areas protected by entry controls and procedures to ensure that only authorized personnel have access.	Access Control; Physical Security	Access to the server room is restricted to authorized staff only.
PE-3	Physical security and procedures for offices, rooms, and facilities.	Access Control; Governance and Risk Management; Physical Security	Staff lock doors that allow access to PCS assets. Security guards inspect doors to make sure they are locked properly.
PE-4	Physical protection against fire, flood, earthquake, explosion, civil unrest, etc.	Access Control; Physical Security	Fire suppression unit installed around critical equipment.
PE-5	Physical security and procedures for working in secure areas.	Access Control; Physical Security	Documentation for physical security procedures is included with new employee training and reviewed at regular training events.
PE-6	Physical security and procedures for mail rooms, loading areas, etc., established. These areas must be isolated from PCS enterprise system areas.	Access Control; Physical Security	Server room and PLC cabinets are isolated from areas that delivery personnel and customers may visit.
PE-7	Physical security and procedures against equipment environmental threats and hazards or unauthorized access.	Physical Security	The utility monitors facilities using security cameras.
PE-8	Physical/logical protection against power failure of equipment UPS.	Physical Security; Service Level Agreements	Uninterruptible power supplies (UPS) are available as power backup for critical components.
PE-9	Physical/logical protection against access to power and telecommunications cabling established.	Physical Security	A utility has a standby power source with separated power cabling for critical sites.

PM: Program Management & Security Assessment and Authorization		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
PM-1	Asset management program including a repository containing all significant assets of the organization with a responsible party for each, periodic inventories, and audits.	Governance and Risk Management; Cyber-Informed Engineering	A database is used to keep track of building conditions in the facility.
PM-2	Policies and procedures for acceptable use of assets and information approved and implemented.	Governance and Risk Management;	PLCs that cannot update past a specific security revision are not acceptable for use in the PCS.
PM-3	Centralized logging system including policies and procedures to collect, analyze and report to management.	Telecommunications, Network Security, and Architecture; Governance and Risk Management;	A utility has a network intrusion detection system (NIDS) to monitor network traffic.
PM-4	SLAs for software and information exchange with internal/external parties in place including interfaces between systems and approved policies and procedures.	SLAs; Governance and Risk Management	Third parties must review and sign an information exchange policy before connecting to the system.
PM-5	Data classification policies and procedures for handling and labeling based on confidentiality and criticality approved and implemented.	Governance and Risk Management	A third-party system integrator asks the SCADA tech to email a document with sensitive network information. The SCADA tech refuses and notifies the integrator of the secure file transfer system in place.

PS: Personnel Security		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
PS-1	Policies and procedures for hiring/terminating processes on employees, contractors, or support companies to include background checks and contract agreements approved and implemented.	Governance and Risk Management; Personnel Security	A background check on employees is required before they may be given access to the PCS system.
PS-2	Defined and approved security roles and responsibilities of all employees, contractors and third-party users.	Governance and Risk Management; Personnel Security	A company policy is in place limiting the access of third-party users to assets, systems, and data.
PS-3	A clear desk policy in place including clear papers, media, desktop, and computer screens.	Governance and Risk Management; Personnel Security	Confidential documents are stored in locked file cabinets when not in use, as required by policy.
PS-4	Disciplinary process for security violations established.	Governance and Risk Management; Personnel Security	An operator who props open doors to critical areas could face disciplinary action as outlined in the utility's policies and procedures.

RA: Risk Assessment		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
RA-1	Risk assessment and approval process before granting access to the organization's information systems.	Governance and Risk Management	A third-party system integrator would need to contact IT before connecting to the system's network.
RA-2	Third party agreement process to ensure security on access, processing, communicating, or managing the organization's information or facilities.	Governance and Risk Management; SLAs	System integrators can only access the facility's equipment remotely from a Virtual Private Network (VPN) connection.
SA: System and Services Acquisition		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
SA-1	Authorization process established for new systems or changes to existing information processing systems.	Governance and Risk Management	A change management/review process is used to evaluate suggested changes to facility.
SA-2	Change controls of systems development, outsourced development, system modification, and testing established, including acceptance criteria for new systems, monitoring of internal/outsourced development, and control of system upgrades.	Governance and Risk Management; SLAs	A third-party system integrator is preparing to make changes to SCADA software. The SCADA tech requires the integrator to follow the change procedure and test the changes in a sandbox environment before they are deployed in production.
SA-3	Change controls of operating systems, network configuration/topology, network security established, including changes to IDS/IPS, traffic control/monitoring, new systems, and system upgrades.	Governance and Risk Management; Server and Workstation Hardening	Automatic updates to the operating system are disabled, but monthly manual updates are reviewed and applied in coordination with operations.
SA-4	Risk based mobility policies and procedures established to protect against inherent risk of mobile computing and communication systems.	Operations Security; Governance and Risk Management	Remote access is restricted to only the most necessary applications and only allowed through secure measures.
SA-5	Periodic review of backup policies and procedures and testing of recovery processes.	Governance and Risk Management	System backups are tested on a regular basis by completing a system restoration to the test environment.
SI: System and Information Integrity		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
SI-1	Electronic commerce infrastructure in place providing integrity, confidentiality and non-repudiation and including adherence to pertinent laws, regulations, policies, procedures, and approval by management.	Governance and Risk Management	The company selected to perform billing is compliant with pertinent laws, regulations, policies and procedures that are relevant to the utility.
SI-2	System acceptance standards including data validation (input/output), message authenticity, and system integrity established to detect information corruption during processing.	Governance and Risk Management	Acquired assets are inspected, assessed, and documented before implementation with existing systems.

SI-3	Interactive system for managing password implemented to ensure password strength.	Access Control; Application Security	When configuring a new user's password, it must meet minimum character length requirements.
SI-4	Organization-wide clock synchronization system in place.	Telecommunications, Network Security, and Architecture	All managed network devices synchronize their clocks to a known good source.
SI-5	Privileged programs controls established to restrict usage of utility programs that could reset passwords or override controls as well as enterprise system audit tools that can modify or delete audit data.	Application Security; Telecommunications, Network Security, and Architecture	Utility has implemented tiered access so non-administrator users are unable to make changes to system security settings.
DS: Data Security		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
DS-1	A program established to ensure compliance with the minimum PCI requirements for your associated level.	Governance and Risk Management; Data Security	The company selected to perform billing is compliant with the minimum PCI requirements for the utility's associated level.
DS-2	A Privacy Policy as well as a Cyber Security Breach Policy are implemented.	Business Continuity and Disaster Recovery; Governance and Risk Management; Data Security	An operator knows how to identify and respond to a suspected cyber breach, based on their cybersecurity training.
DS-3	A program is established to ensure compliance with the minimum HIPAA requirements. Develop a Privacy Policy as well as a Cyber Security Breach Policy.	Business Continuity and Disaster Recovery; Governance and Risk Management; Data Security	Current practices are reviewed by legal counsel for legal compliance with HIPAA.
CIE: Cyber-Informed Engineering		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
CIE-1	A program is in place to engage engineering staff in understanding and mitigating high-consequence and constantly evolving cyber threats throughout the engineering life-cycle including: design, implementation, maintenance, and decommissioning.	Cyber-Informed Engineering	Engineering staff is fully aware of the potential for a cyber breach. They design electrical and mechanical systems to provide functionality in the case of a SCADA system compromise.
SU: Supply Chain		***Cybersecurity Practice Areas/ Recommended Projects***	***Additional Details***
SU-1	A supply chain risk management program.	Governance and Risk Management	Chain of custody documentation is required for all chemicals used in treatment.
SU-2	A supply chain risk management program that includes cybersecurity.	Governance and Risk Management	Preferred vendors for computer hardware, software and peripherals are identified and selected based on evaluation of their supply chain among other criteria.

SC: System and Communications Protection		Cybersecurity Practice Areas/ Recommended Projects	Additional Details
SC-1	Policies and procedures governing cryptography and cryptographic protocols including key/certificate-management established to maximize protection of systems and information.	Governance and Risk Management	When selecting new PLCs for a system upgrade, SCADA techs evaluate the option of using newer PLCs that offer encryption for communication.
SC-2	Centralized authentication system or single sign-on established to authorize access from a central system.	Access Control; Application Security	Operators have one username and password for PCS equipment which is managed from a central system.
SC-3	Policies and procedures established for network segmentation including implementation of DMZs based on type and sensitivity of equipment, user roles, and types of systems established.	Governance and Risk Management	All external communication with the PCS is implemented via DMZ.
SC-4	Intrusion detection, prevention, and recovery systems including approved policies and procedures established to protect against cyber-attacks. System includes repository of fault logging, analysis, and appropriate actions taken.	Governance and Risk Management; Telecommunications, Network Security, and Architecture	Within the SCADA system network, vendor systems are placed on a separate subnet.
SC-5	Anomaly based IDS/IPS established including policies and procedures.	Telecommunications, Network Security, and Architecture	The IT tech monitors IDS system exception logs daily to determine if ongoing attacks are occurring and works with SCADA tech to address any issues.
SC-6	Network management and monitoring established including deep packet inspection of traffic, QoS, port-level security, and approved policies and procedures.	Governance and Risk Management; Telecommunications, Network Security, and Architecture	An actively managed firewall is in place to allow secure data transfer via DMZ to provide operations data to utility asset managers.
SC-7	Information exchange protection program in place to protect data in-transit through any communication system including the Internet, email, and text messaging and approved policies and procedures.	Governance and Risk Management; Telecommunications, Network Security, and Architecture	When selecting new PLCs for a system upgrade, SCADA techs evaluate the option of using newer PLCs that offer encryption for communications.
SC-8	Routing controls established to provide logical separation of sensitive systems and enforce the organization's access control policy.	Operations Security; Telecommunications, Network Security, and Architecture	Within the SCADA system network, vendor systems are placed on a separate subnet rather than being on a single "flat" network.
SC-9	Process isolation established to provide a manual override "air gap" between highly sensitive systems and regular environments.	Operations Security; Telecommunications, Network Security, and Architecture	A utility will physically separate a pump station from any sort of information transfer from any other network. This however is only a true air gap when there is absolutely no information transfer. If information is transferred though a DMZ or firewall that would not be an example of this control. In that scenario select this control as "Not Planned and/or Not Implemented - Risk Accepted".

SC-10	Program for hardening servers, workstations, routers, and other systems using levels of hardening based on criticality established. Program should include policies and procedures for whitelisting (deny-all, allow by exception).	Server and Workstation Hardening; Governance and Risk Management	Ports are disabled for all network devices when not in use.
SC-11	Framework for hardening of mobile code and devices established (including acceptance criteria and approved policies and procedures).	Server and Workstation Hardening; Governance and Risk Management	A water utility chooses to not allow personal mobile devices to connect to the control network. The utility does provide mobile devices managed by IT that can connect to the network.
SC-12	Remote access framework including policies and procedures established to provide secure access to telecommuting staff, established for the management, monitoring, review, and audit of remote access to the organization.	Access Control; Governance and Risk Management	Remote access to the SCADA system requires two factor-authentication.
SC-13	Testing standards including test data selection, protection, and system verification established to ensure system completeness.	Governance and Risk Management	Organization has a FAT procedure that requires vendors to demonstrate security of systems before they are purchased.
SC-14	Network segregation. Firewalls, deep packet inspection and/or application proxy gateways.	Operations Security; Telecommunications, Network Security, and Architecture	"Whitelisting" of network components is done to manage data transfer between and within network segments.
SC-15	Logically separated control network. Minimal or single access points between corporate and control network. Stateful firewall between corporate and control networks filtering on TCP and UDP ports. DMZ networks for data sharing.	Operations Security; Telecommunications, Network Security, and Architecture	An actively managed firewall is in place to allow secure data transfer via DMZ to provide operations data to utility asset managers.
SC-16	Defense-in-depth. Multiple layers of security with overlapping functionality.	Operations Security; Telecommunications, Network Security, and Architecture	A utility employs multiple types of physical and cybersecurity efforts to protect assets and systems. The efforts include such things as locking doors, physical access control, and unique login requirements for each staff member.
SC-17	Virtual Local Area Network (VLAN) for logical network segregation.	Telecommunications, Network Security, and Architecture	Within the SCADA system network, vendor systems are on a separate subnet.
SC-18	Minimize wireless network coverage.	Telecommunications, Network Security, and Architecture	Tests are conducted regularly to determine if the WiFi signals reach outside the intended area of use. If the signal reaches outside the intended area, the signal is turned down accordingly.
SC-19	802.1X user authentication on wireless networks.	Telecommunications, Network Security, and Architecture	No "open" WiFi connections are allowed.
SC-20	Wireless equipment located on isolated network with minimal or single connection to control network.	Telecommunications, Network Security, and Architecture	WiFi equipment in the plant does not connect directly to SCADA network.
SC-21	Unique wireless network identifier SSID for control network.	Telecommunications, Network Security, and Architecture	The WiFi for the control system has a unique SSID from the business network.

SC-22	Separate Microsoft Windows domain for wireless (if using Windows).	Telecommunications, Network Security, and Architecture	A wireless LAN specific domain controller is in place.
SC-23	Wireless communications links encrypted.	Encryption; Telecommunications, Network Security, and Architecture	All data transferred via the wireless network is encrypted using current wireless communication best practices.
SC-24	Communications links encrypted.	Encryption; Telecommunications, Network Security, and Architecture	All data transferred via the wired network is encrypted using current wireless communication best practices.
SC-25	VPN using IPsec, SSL or SSH to encrypt communications from untrusted networks to the control system network.	Encryption; Telecommunications, Network Security, and Architecture	An operator who can access the system remotely must do so through a secured VPN client configuration.

Appendix F: Cross Reference to NIST 1.1 Cybersecurity Framework

The following table provides a cross-reference between the Cybersecurity Controls incorporated into the AWWA Cybersecurity Guidance Tool and the Framework Core (Appendix A) included in the Cybersecurity Framework issued by NIST on April 16, 2018.

Function	Category	Sub-Category	Description	AWWA Guidance Control
IDENTIFY	Asset Management	ID.AM-1	Physical devices and systems within the organization are inventoried	PM-2
		ID.AM-2	Software platforms and applications within the organization are inventoried	PM-2
		ID.AM-3	Organizational communication and data flows are mapped	PM-2
		ID.AM-4	External information systems are catalogued	MA-3
		ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	PM-5
		ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	PE-4, PS-2
	Business Environment	ID.BE-1	The organization's role in the supply chain is identified and communicated	RA-2, PS-2, CM-5
		ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	MA-2
		ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	IR-2
		ID.BE-4	Dependencies and critical functions for delivery of critical services are established	IR-2
		ID.BE-5	Resilience requirements to support delivery of critical services are established	IR-3
	Governance	ID.GV-1	Organizational information security policy is established	IR-2, AU-2
		ID.GV-2	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	PS-2, AU-4, AU-6
		ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	IR-3
		ID.GV-4	Governance and risk management processes address cybersecurity risks	AU-3, AU-5, CM-6
	Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented	AU-5, RA-1, IR-2
		ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources	AU-5, PM-3, IR-2

Function	Category	Sub-Category	Description	AWWA Guidance Control
IDENTIFY – cont'd		ID.RA-3	Threats, both internal and external, are identified and documented	AU-5, RA-1, IR-2
		ID.RA-4	Potential business impacts and likelihoods are identified	AU-5, RA-1, IR-2
		ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	AU-5
		ID.RA-6	Risk responses are identified and prioritized	IR-1
	Risk Management Strategy	ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	IR-2
		ID.RM-2	Organizational risk tolerance is determined and clearly expressed	SA-4
		ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	SC-4
	Supply Chain Risk Management	ID.SC-1:	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	SU1
		ID.SC-2:	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	SU2
		ID.SC-3:	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	SU2
		ID.SC-4:	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations	SU1
PROTECT	Access Control	PR.AC-1	Identities and credentials are managed for authorized devices and users	IA-1, RA-1, SC-19
		PR.AC-2	Physical access to assets is managed and protected	PE-1, PE-2, PE-3
		PR.AC-3	Remote access is managed	IA-7, SC-12, SC-18, SC-21, RA-2
		PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties	IA-3, SC-22
		PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate	SC-8, SC-9, SC-14, SC-15, SC-16, SC-17, SC-20, SC-25