Enterprise Resiliency Business Practice Benchmarking

The purpose of this guide is to assist to water and wastewater utilities in improving their resiliency performance using business practice benchmarking. This guide was originally developed by the American Water Works Association Utility Benchmarking Advisory Committee for conducting a resiliency benchmarking workshop at the 2019 AWWA Water Infrastructure Conference. This guide is a companion to the Utility Resilience Benchmarking Index Worksheet also developed for the conference workshop and available at swefc.unm.edu/home/resource/utility-resilience-benchmarking-index-worksheet.

The four measures in this guide are a part of the resiliency measures found in the AWWA Utility Benchmarking Survey. Information on the survey can found at www.awwa.org/benchmarking. The purpose of these practice benchmarking measures is to facilitate discussion for utilities in determining their current performance and a better understanding of leading practices in order to determine further targets for performance improvement.

The two-dimensional matrix used for these exercises originated from Water Research Foundation "benchmarking tool." The tool can be downloaded at www.waterrf.org/research/projects/performance-benchmarking-effectively-managed-water-utilities. The benchmarking tool contains more benchmarking measures especially for enterprise resiliency. This guide uses leading practices from the EPA Sustainable Guidance Roadmap (EPA Roadmap) found at www.epa.gov/sustainable-water-infrastructure/moving-toward-sustainability-sustainable-and-effective-practices. The benchmarking measures used in this guide are a combination of the WRF benchmarking tool framework with the more current leading practices from the EPA Roadmap. The Cybersecurity Preparedness measure was developed based on the National Institute of Standards and Technologies Cybersecurity Framework.

For each benchmarking measure, utilities should discuss their current performance and implementation level and identify the intersection of the two components and write "Current" in the box. In evaluating future targets, utilities will need to determine their next performance/implementation levels. This should be done with utility subject matter experts and leadership to ensure that all teams members agree or come to consensus on the future target performance level. In many cases, it will be one to two years in order to achieve the target performance. The target should not be set at the highest level without consideration to the time period of achievement. The key is to develop manageable targets that are achievable and allow employees to feel a sense of accomplishment for reaching their targets.

There are four enterprise resiliency practice benchmarking measures:

- Recovery & Mitigation
- Emergency Response Planning
- Risk Assessment and Response Preparedness
- Cybersecurity Preparedness

Attribute: Enterprise Resiliency **Performance Measure: Recovery & Mitigation**					
The purpose of this measure is to ensure that the utility has mitigation and recovery plans and activities with adequate funding for projects. *See examples on next page on Level of Performance Achieved*		Level of Performance Achieved			
		No Plan in Place	General awareness of mitigation and recovery activities, projects, and funding is in place for efficient system and services restoration.	Implementation of mitigation and recovery activities, projects, and funding is in place.	Ability to recover from a full suite of incidents through implementation of comprehensive mitigation and recovery activities, projects, and funding is in place
Degree of Implementation	Recovery & Mitigation covers only a few business areas of the utility (50% or less); risk mitigation plans are not monitored				
	Recovery & Mitigation covers only a few business areas of the utility (50% or less); and, risk mitigation plans are monitored infrequently				
	Recovery & Mitigation covers most business areas of the utility (50-75%); and, risk mitigation plans are monitored infrequently				
	Recovery & Mitigation covers most business areas of the utility (50-75%); and, risk mitigation plans are monitored regularly				
	Recovery & Mitigation covers all business areas of the utility (100%); and, risk mitigation plans are monitored regularly				

Guidelines for Performance (based on Enterprise Resiliency Attribute of EPA's "Moving Toward Sustainability" Roadmap Guide)

1. No Plan in Place
2. General awareness of mitigation and recovery activities, projects, and funding is in place for efficient system and services restoration.
   - Local and state officials identified that would be involved in recovery (e.g., local community planners and State Hazard Mitigation Officers).
   - Local and state official coordination (e.g., local community planners and State Hazard Mitigation Officers).
   - Understand options for resilient projects, concepts, and strategies, such as flood-proofing and relocating at-risk assets.
   - Awareness of the required documentation and application processes for federal funding programs.
3. Implementation of mitigation and recovery activities, projects, and funding is in place.
   - Recovery plan (developed through collaborations with local and state officials that would be involved in recovery, including establishing clear roles and responsibilities for key partners such as local community planners and State Hazard Mitigation Officers).
   - Retainer contracts with consultants and backup equipment acquisition.
   - Business preparedness and continuity plan (developed, tested, and maintained to continue basic business operations during and immediately after disruptive events).
   - SOPs for documenting pre- and post-disaster condition of key assets applying for the federal funding program.
   - Key resilient projects, concepts, and strategies implementation, such as flood-proofing and relocating assets at risk from extreme weather events.
4. Ability to recover from a full suite of incidents through implementation of comprehensive mitigation and recovery activities, projects, and funding is in place.
   - Prepared to conduct long-term public health and environmental health monitoring after a contamination incident.
   - Advanced contracts and agreements to support continuity plan implementation when needed.
   - Detailed decontamination decision-making framework (established for remediation/cleanup).
   - Remediation techniques and remedial process for treatment works and contamination distribution/collection systems implementation ability.

Instructions

Mark "C" in the box for Current performance and implementation achieved

Mark "T" in the box for Target performance and implementation desired

Attribute: Enterprise Resiliency **Performance Measure: Emergency Response Planning**					
The purpose of this measure is to ensure that the utility has emergency response plans, policies and procedures to respond to incidents. *See examples on next page on Level of Performance Achieved*		Level of Performance Achieved			
		No Plan in Place or has not been updated in 10 Years	Emergency Response Plan (ERP) is developed containing basic policies and procedures.	The ERP is enhanced with additional capabilities and supported through more structured relationships with potential response partners.	ERP is enhanced with incident-specific Emergency Action Procedures (EAPs) for responding to a specific type of incident, and enhanced capability to test, exercise, and to refine the Emergency Response Plan is in place. Ability to respond to a full suite of unexpected events by implementing a comprehensive ERP.
Degree of Implementation	Employees have not been trained in emergency response and recovery				
	Less than 50% of appropriate employees have been trained in emergency response and recovery				
	50% to 100% of appropriate employees have been trained in emergency response and recovery				
	Employee training extends to desktop exercises and simulations				
	Employee training extends to full field test of plans, exercises and training				

Guidelines for Performance (based on Enterprise Resiliency Attribute of EPA's "Moving Toward Sustainability" Roadmap Guide)

1. No Plan in Place
2. Emergency Response Plan is developed containing basic policies and procedures.
   - Basic system information documentation (e.g., system maps and drawings) stored in secure on-site and off-site locations.
   - Emergency roles and responsibilities identification for utility personnel and local response partner agencies (e.g., law enforcement, fire, laboratories, public health agencies, and emergency management agencies).
   - General communication procedures (e.g., who activates the plan, order of notification, and contact information).
   - Training and exercise plan (to identify strategic goals and priorities for training and exercises).
   - Key utility response personnel training (in Incident Command System (ICS) and a plan to implement ICS during an emergency).
   - Critical customer needs and requirements identification and associated response protocols.
3. The Emergency Response Plan is enhanced with additional capabilities and supported through more structured relationships with potential response partners.
   - Alternate water source identification and alternate water supply distribution plans.
   - Mutual aid agreements (e.g., partnerships with neighboring systems for emergency response planning, participation in Water and Wastewater Agency Response Network (WARN), membership in an integrated nationwide network of laboratories such as the Water Laboratory Alliance).
   - Risk communication procedures for issuing messages during an emergency.
   - Business continuity plan (for maintaining solid operations–financially, managerially, and functionally–after any incident).
   - Routine joint training with neighboring utilities and response partners (e.g., full-scale exercises, mutual aid response/requests).
   - Utility representation in local Emergency Operations Center.
   - Response resources organized according to the AWWA resource typing manual.
4. Emergency Response Plan is enhanced with incident-specific Emergency Action Procedures (EAPs) for responding to a specific type of incident, and enhanced capability to test, exercise, and to refine the Emergency Response Plan is in place. Ability to respond to a full suite of unexpected events by implementing a comprehensive Emergency Response Plan.
   - Specific EAP's for incidents such as 1) Severe weather response (e.g., snow, ice, temperature, lightning, flooding, hurricane, tornado); 2) Fire response; 3) Electrical power outage response; 4) Water supply interruption response; 5) Earthquake response; or 6) Disgruntled employee response.
   - Reviewed and updated utility response plans based on training and exercise activities (e.g., operations-based drills, functional and full-scale exercises), operational changes, and lessons learned from emergencies
   - Capability to respond to mutual aid requests in self-sufficient manner, including cross-training staff to support neighboring utilities in the event of a mutual aid request.
   - Integrated consequence management plans as part of a Water Quality Surveillance and Response System for responding to contamination within the distribution system.
   - Interstate mutual aid request response plan (through Emergency Management Assistance Compact).

Instructions

Mark "C" in the box for Current performance and implementation achieved

Mark "T" in the box for Target performance and implementation desired

Attribute: Enterprise Resiliency **Performance Measure: Risk Assessment and Response Preparedness**					
The purpose of this measure is to ensure that the utility has the appropriate risk assessment and response preparedness to address emergent threats and risks. *See examples on next page on Level of Performance Achieved*		Level of Performance Achieved			
		No Plan in Place; no risk assessment conducted in last 10 Years	Risks to high-consequence assets are identified and reduced.	Increase capacity to understand and detect threats to the system, risks to all major assets are identified and reduced, and all hazards risk management needs are fully integrated into broader utility planning and investment activities.	Emergent risks to all major assets are consistently addressed. Proactive and specialized shifts in operational procedures and updated capital investment criteria are changed when necessary.
Degree of Implementation	Risk assessment covers only a few business areas of the utility (50% or less); and, risk reduction plans are not developed or monitored				
	Risk assessment covers only a few business areas of the utility (50% or less); and, risk reduction plans are monitored infrequently				
	Risk assessment covers most business areas of the utility (50-75%); and, risk reduction plans are monitored infrequently				
	Risk assessment covers most business areas of the utility (50-75%); and, risk reduction plans are monitored regularly				
	Risk assessment covers all business areas of the utility (100%); and, risk reduction plans are monitored regularly				

Guidelines for Performance (based on Enterprise Resiliency Attribute of EPA's "Moving Toward Sustainability" Roadmap Guide)

1. No Plan in Place
2. Risks to high-consequence assets are identified and reduced.
   - Risk assessment for high-consequence assets (i.e., those that would result in high public health or economic impacts if damaged).
   - Risk reduction plan containing countermeasures with prioritized list of mitigation projects (i.e., near- or long-term capital improvement projects).
   - Low-cost or near-term process improvement projects (e.g., fences and barriers around key utility facilities and infrastructure; doors and gates routinely locked; chemicals stored safely and securely, and properly disposed of; video cameras, especially on gates and sensitive areas within the treatment plant, such as those where chemicals are stored; computers and network systems protected with passwords, and passwords changed routinely; abnormal conditions or activities reported by personnel; employee training in basic workplace safety practices and to actively monitor for abnormal or threatening situations and activities).
   - Resilience measures (e.g., flood threats understood and practical mitigation options identified to protect critical assets).
3. Increase capacity to understand and detect threats to the system, risks to all major assets are identified and reduced, and all hazards risk management needs are fully integrated into broader utility planning and investment activities.
   - Risk assessment for all major assets including assessments of consequences and failure potential.
   - Risk reduction plan with a prioritized list of risk mitigation projects that, if fully implemented, would achieve acceptable risk levels for all major assets (e.g., hardening for facilities vulnerable to security threats and natural disasters; electronic files and network systems regularly backed up; chemical delivery control; intruder detection systems).
   - Risk reduction plan integration with long-range and capital investment planning for other projects.
   - Understanding regional environmental risks (e.g., fires, floods, earthquakes, tornados) and their relationship to utility operations and infrastructure (updated and maintained as current).
   - Identification and analysis of a wide range of contaminants and their properties (e.g., through the Water Contamination Information Tool).
   - Continuous on-line instrumentation for establishing trends and detecting abnormal occurrences (e.g., for pH and chlorine) in the water distribution system.
4. Emergent risks to all major assets are consistently addressed. Proactive and specialized shifts in operational procedures and updated capital investment criteria are changed when necessary.
   - Monitor/scan proactively for modern and emergent threats, and real-time monitoring for threat progression (e.g., watershed monitoring networks that support progressive storm alert systems).
   - Integrated Water Quality Surveillance and Response System addressing potential contamination within the distribution system.
   - Regular research on emerging trends that could pose new threats to the system, including changing weather patterns (i.e., climate change risk assessment integrated into existing risk assessment and reduction plan) and contamination threats.
   - Diversification and redundancy for critical supply, distribution, and treatment functions (e.g., emergency interconnects or bulk loading stations).

Instructions

Mark "C" in the box for Current performance and implementation achieved

Mark "T" in the box for Target performance and implementation desired

Attribute: Enterprise Resiliency **Performance Measure: Cybersecurity Preparedness**				
The purpose of this measure is to ensure that the utility has established appropriate cybersecurity plans and practices to reduce threats. *See examples on next page on Level of Performance Achieved and on Degree of Implementation of Tiers*	Level of Performance Achieved			
	No Plan in place	Utility has identified and established a basic cybersecurity plan and is minimally implemented.	Utility has developed a cybersecurity plan, that has been approved and generally used throughout facility. Utility is tracking Risk Scores in the NIST CSF Five Function areas.	Utility has established and fully incorporated a detailed cybersecurity plan which is routinely reviewed and implemented. Utility is tracking and setting targets for improvement in Five Function areas.
Degree of Implementation: NIST CSF Tier 1 Partial				
Degree of Implementation: NIST CSF Tier 2 Risk Informed				
Degree of Implementation: NIST CSF Tier 3 Repeatable				
Degree of Implementation: NIST CSF Tier 4 Adaptive				

Instructions

Mark “C” in the box for Current performance and implementation achieved
Mark “T” in the box for Target performance and implementation desired

National Institute of Standards and Technologies (NIST) Cybersecurity Framework (CSF) Tiers
Source: https://www.nist.gov/cyberframework/framework

Level of Performance Achieved

NIST CSF Framework Core consists of five high level functions. Utilities can contact a self-assessment in each level below and obtain risk scores and evaluate performance gaps for improvement.

Identify: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Protect: Develop and implement appropriate safeguards to ensure delivery of critical services.
Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

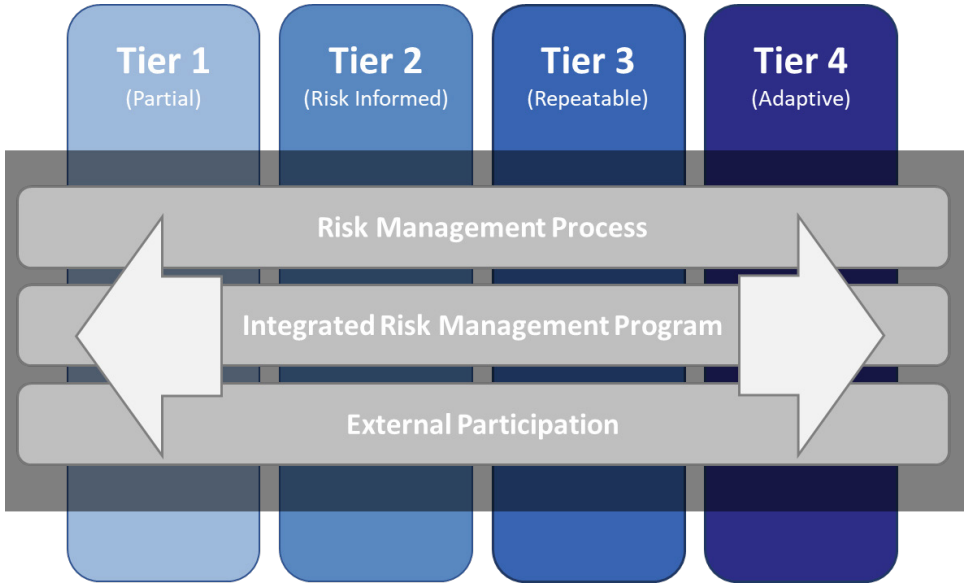
Degree of Implementation

NIST CSF Tiers and Processes

Risk Management Process: The functionality and repeatability of cybersecurity risk management

Integrated Risk Management Program: The extent to which cybersecurity is considered in broader risk management decisions

External Participation: The degree to which the organization benefits my sharing or receiving information from outside parties



The NIST CSF Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management processes, how well integrated cyber risk decisions are into broader risk decisions, and the degree to which the organization shares and receives cybersecurity information from external parties.

Tier 1 – Partial	Tier 2 – Risk Informed	Tier 3 – Repeatable	Tier 4 – Adaptive
▪ Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements. ▪ There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization. ▪ The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.	▪ Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements. ▪ There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable or reoccurring. ▪ Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses but does not act consistently or formally upon those risks.	▪ The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape. ▪ There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. ▪ The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities.	▪ The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats. ▪ There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. ▪ The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses.