Mirazon®

CHECKLIST

Utility Cybersecurity & Resilience Checklist

Protect Critical Infrastructure. Reduce Risk. Strengthen Resilience.

www.mirazon.com | (502) 240-0404 | info@mirazon.com

How Prepared Is Your Utility Environment?

Cybersecurity isn't just about stopping threats. For utility providers, it's about keeping operations running, supporting your team, meeting regulatory expectations, and delivering reliable service to the communities that count on you every day.

The challenge is that maintaining all of that has become more complicated. Many utility organizations are balancing aging infrastructure, growing technology demands, third-party vendor relationships, and an evolving threat landscape—all while trying to keep critical systems running smoothly.

That's where this checklist comes in.

Use it as a straightforward way to evaluate your current environment, identify potential gaps, and uncover opportunities for improvement. You don't need to tackle everything at once. Sometimes the biggest wins come from small changes or initiatives that have been sitting on the back burner.

Whether you're looking to strengthen cybersecurity, support operational reliability, improve recovery readiness, or simply understand where you stand today, this checklist can help you start the conversation and build a stronger foundation for the future.

Secure Your Network & Infrastructure

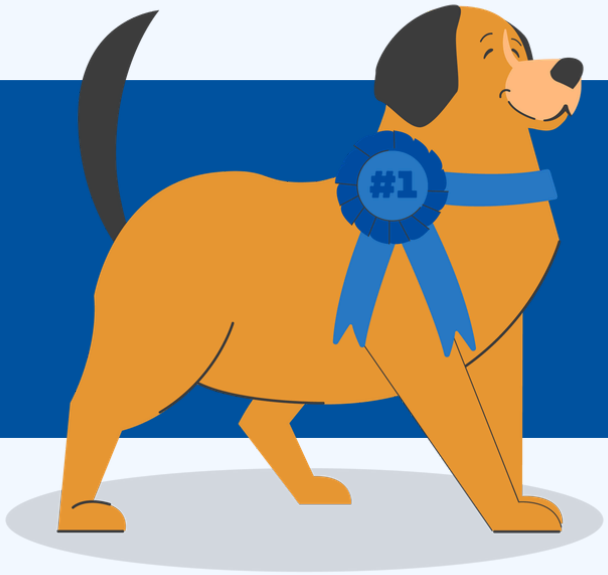
- [ ] Segment operational systems from business systems
- [ ] Separate SCADA, OT, and IT environments where appropriate
- [ ] Review firewall rules regularly and remove unnecessary access
- [ ] Secure remote access connections with Multifactor Authentication (MFA)
- [ ] Keep network equipment, firewalls, and security appliances updated
- [ ] Regularly monitor network activity for unusual behavior
- [ ] Identify and remove unsupported or end-of-life hardware where possible

Manage Legacy Systems Responsibly

- [ ] Maintain an inventory of legacy devices, systems, and applications
- [ ] Document which systems are critical to operations
- [ ] Restrict internet access for unsupported systems whenever possible
- [ ] Implement additional controls such as segmentation and enhanced monitoring
- [ ] Create a long-term modernization plan for aging infrastructure
- [ ] Review legacy systems annually to evaluate risk and replacement priorities

PRO TIP:

Just because a system is old doesn't mean it's a problem. The key is understanding where the risks are and putting the right protections in place so you can operate confidently while planning for the future.



Strengthen Access Controls

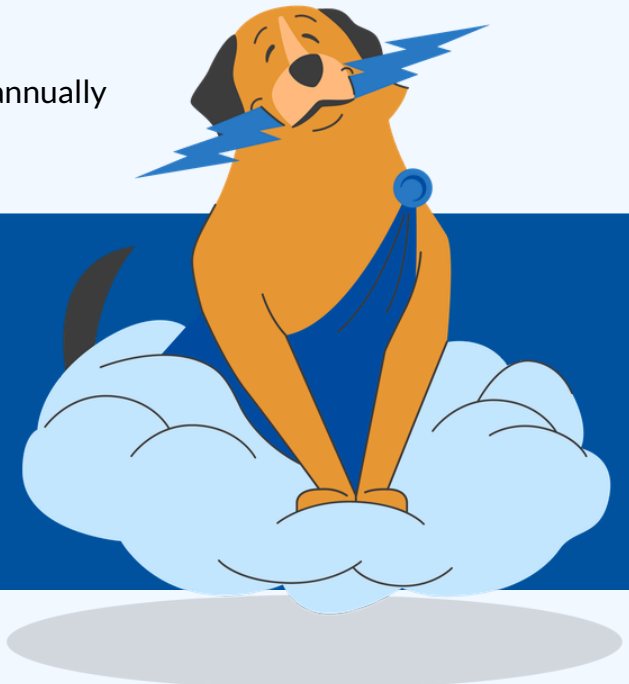
- [ ] Apply the principle of least privilege (POLP)
- [ ] Review user permissions regularly
- [ ] Remove inactive or unused accounts promptly
- [ ] Require strong password policies
- [ ] Enable Multifactor Authentication (MFA) for all critical systems
- [ ] Monitor administrator and privileged accounts
- [ ] Review vendor and third-party access on a regular basis
- [ ] Establish a documented process for granting and removing access

Protect Your Data

- [ ] Back up critical systems and operational data regularly
- [ ] Follow the 3-2-1 Backup Rule
- [ ] Verify that critical data can be recovered through routine backup testing
- [ ] Encrypt sensitive data when it's stored and when it's being sent or shared
- [ ] Document recovery objectives for critical systems
- [ ] Ensure backup procedures are reviewed and updated annually

PRO TIP:

Having backups is a great start, but knowing they can be restored is what really matters. Regular recovery testing helps reduce uncertainty and ensures you're ready when every minute counts.



Prepare for Cyber Incidents

- [ ] Maintain a documented incident response and disaster recovery plan
- [ ] Clearly define internal roles and responsibilities
- [ ] Keep emergency contacts updated
- [ ] Include critical vendors and partners in response planning
- [ ] Conduct tabletop exercises annually
- [ ] Document communication procedures for customers, employees, and stakeholders
- [ ] Review lessons learned after incidents or drills

Turn Employees Into Your First Line of Defense

- [ ] Provide ongoing cybersecurity awareness training
- [ ] Conduct phishing simulations throughout the year
- [ ] Train employees on reporting suspicious activity
- [ ] Educate users on password security and Multifactor Authentication (MFA)
- [ ] Teach employees to protect physical access to buildings, devices, and sensitive information
- [ ] Make security part of onboarding and annual training programs
- [ ] Encourage a culture where employees feel comfortable reporting concerns

PRO TIP:

Technology can block many threats, but informed employees often stop the ones technology misses. The more aware and engaged your team is, the better positioned your organization will be to identify issues early and reduce unnecessary risk.

Improve Visibility & Monitoring

- [ ] Monitor critical systems and infrastructure continuously
- [ ] Review logs and security alerts regularly
- [ ] Conduct regular security assessments
- [ ] Track asset inventories and system changes
- [ ] Establish alerting for unusual or unauthorized activity
- [ ] Document remediation efforts and corrective actions
- [ ] Regularly review security metrics with leadership

Support Compliance & Governance

- [ ] Review applicable regulatory requirements annually
- [ ] Maintain current cybersecurity policies and procedures
- [ ] Document security controls and system configurations
- [ ] Perform internal compliance reviews
- [ ] Track security risks and mitigation efforts
- [ ] Ensure third-party vendors meet security expectations
- [ ] Review disaster recovery and business continuity plans annually

REMINDER:

Compliance is an important milestone, but checking a box isn't the end goal. The real value comes from building a secure, resilient environment that helps protect critical systems, support reliable operations, and give your team confidence moving forward.

How Do You Measure Up?

40+ Checks

You're in a strong position. Keep building on that momentum by regularly reviewing your environment, testing your plans, and looking for opportunities to strengthen reliability and reduce risk before issues arise.

25-39 Checks

You're on the right track, but there's still room for improvement. Focusing on a few key areas now can help strengthen your security posture, improve resilience, and prepare your organization to respond when unexpected challenges arise.

Under 25 Checks

Don't panic. Every organization starts somewhere. Use this checklist as a roadmap to identify priorities, focus on the biggest risks first, and take practical steps toward building a more secure and resilient utility environment.

Need a Trusted Technology Partner?

Cyber threats aren't slowing down, and the technology supporting utility operations continues to grow more complex. The good news is you don't have to navigate those challenges alone.

Contact Mirazon today to start the conversation. Whether you're focused on cybersecurity, disaster recovery, infrastructure modernization, compliance, or long-term technology planning, we're here to help you build a more secure and reliable future.

Contact Us

Mirazon®

www.mirazon.com
(502) 240-0404
info@mirazon.com