SpryPoint

Utility Market Perspective

# You're Not Alone: Why a Mandated Legacy CIS Upgrade is your Hidden Opportunity to Evaluate Modern Alternatives

You're facing a decision crossroad. Your legacy Customer Information System (CIS) provider is mandating a platform upgrade due to security risks, vulnerabilities, and obsolescence after years of minimal innovation and diminishing customer service.

Unfortunately, simply upgrading your CIS interface doesn't guarantee modernization, especially when the experience, data silos, and workflow constraints remain the same.

These out-of-cycle, time-consuming, and expensive upgrade projects place an unnecessary burden on you and your staff. While untimely, it's also an opportunity to reassess whether legacy platform upgrades truly meet immediate and future demands—or if a more modern CIS makes sense as you stare at the significant upgrade requirements from your current provider.

## The risk of delaying your CIS upgrade

Every day you delay your CIS upgrade, you risk the security of your utility's and customers' data. And vendor-mandated upgrades usually mean your current CIS version is no longer receiving the latest updates and enhancements.

Cyberattacks on utilities are rising fast. Reported incidents increased by nearly 70% from 2023 to 2024 (Reuters, 2024), and more than 60% of U.S. utility operators reported being affected in the past year (Semperis, 2025). Those affected have an average breach cost of half a million dollars (Security Magazine, 2025).

And the reputational damage and erosion of trust among customers, public officials, and staff can be difficult—if not impossible—to fully restore.

Furthermore, your legacy CIS isn't keeping up with the compounding set of market realities utilities face today. Customers now expect transparent billing, real-time consumption insights, and easy self-service, just as regulations become more complex. Compliance solves for today, not for tomorrow's requirements.

Moving to a new version of the same architecture with legacy workflows, integrations, and risk is not modernization. In a few years, you may be forced once again to upgrade for the latest security patches and technology enhancements,

So, you're stuck debating whether to take on an untimely CIS upgrade or keep waiting. The resource-intensive preparation, testing, retraining, and disruption from an upgrade can sideline your utility's productivity for months. Waiting may feel less disruptive, but there are real risks to your utility, including security threats and the financial impact they can have.

And even when you're ready to move forward, your legacy CIS providers may lack the capacity to support your timeline as they juggle hundreds of concurrent upgrades, exposing you to even more risks as you wait.

## An alternative option is to consider a modern CIS

Many utility leaders are using these vendor-mandated upgrades as an opportunity to consider a new CIS that delivers automatic, continuous security updates incrementally, without the need for a time-consuming system overhaul. These updates ensure your CIS always has the most up-to-date security features to safeguard your data and latest innovations.

**Legacy CIS upgrade**

- New interface with minimal updates to meet growing demands
- Time-consuming upgrade for every security update
- Security as an afterthought
- Manual Connector Fixes
- Vendor-driven timelines

vs

**Modern CIS**

- Built for how utilities work to meet immediate needs and future demands
- Continuous, automatic security updates without disruption
- Security-first approach
- Productized integrations
- Utility-controlled cadence

SpryPoint is built from the ground up to contend with today's rapid pace of change. A modern CIS is not just about upgrading technology; it is transforming how you work and serve your customers and community. You need a CIS built specifically for how utilities operate to support better customer experiences, more efficient day-to-day operations, and a rapidly evolving industry that requires business visibility and data-driven decision making.

### A modern CIS transforms how you serve customers

**"We're not just upgrading technology, we're improving how we serve our community," said Joe Bryant, who served as lead project manager at the City of West Jordan Water Utility. "This partnership [with SpryPoint] supports better customer experiences, stronger conservation outcomes, and more efficient day-to-day operations as our city continues to grow."**

# Security is foundational to a transformational CIS

Customer trust is foundational to utility relationships. That's why you need a modern CIS like SpryPoint with the highest levels of security and reliability built into the platform and its processes. With a modern CIS like SpryPoint, you reduce security and risk exposure from aging architectures, and shift from reactive fixes to continuous protection.

Consider the following security requirements from a modern, enterprise-ready CIS:

**Scalability and agility**
to scale up or down resources based on demand, ensuring optimal performance and cost management even as your business grows.

**Innovation and speed**
to rapidly develop, test, and deploy new applications and features.

**Reliability and uptime**
using AWS' distributed infrastructure with multiple data centers and availability zones to ensure high availability and minimal downtime.

**Security and compliance**
with strict security standards and certifications, including SOC 2, ensuring that your data is protected and compliant.

**API-first approach**
to add new integrations with ease.

**SCIM and SAML**
user management and authentication.

Transformational CIS systems are cloud-native, so you can quickly and securely accommodate workflow and process changes, as well as new security requirements, without business disruptions or added costs.

Cloud-native CIS platforms enable updates, not upgrades, built into the platform for continuous improvements, rather than the resource-consuming preparation, testing, retraining, and disruption that come with an upgrade. Continuous security updates protect your utility and customer data against the latest threats and are baked into each release, ensuring you remain vigilant.

But most importantly, does your CIS vendor have a security-first approach? A security-first approach prioritizes and proactively considers potential threats as an integral part of the decision-making process for every deployment and update, safeguarding data.

It's a critical process that CIS vendors must offer to provide peace of mind and avoid the reputational harm that could result from a security breach.

# Expect more from your CIS

Change is a constant in the utility industry. Your CIS must evolve at the speed of your business. If you're stuck in a vendor-mandated upgrade cycle, this could be an opportunity to consider an alternative that supports better customer experiences, more efficient day-to-day operations, and greater business visibility for data-driven decision-making.

By choosing a transformational CIS like SpryPoint with built-in future enablers, your next CIS project could be the last one your utility ever needs.

**SpryPoint is a new generation of customer service and operations software that empowers you to do game-changing, transformational work.**

Let's connect