FROM AUDIT TO ASSESSMENT:

How a Municipal Government Built a Strategic Path to Cybersecurity Maturity

APRIL 2026

A JANUS ASSOCIATES CASE STUDY

TEL: +1 203.251.0200

INFO@JANUSASSOCIATES.COM

1200 HIGH RIDGE ROAD STAMFORD, CT 06907

JANUSASSOCIATES.COM

Client

A mid-sized U.S. municipality engaged JANUS Associates seeking an independent cybersecurity audit. Their IT leadership wanted clear visibility into their security posture, gaps, and compliance readiness to safeguard essential public services and meet rising insurance and regulatory expectations.

Challenge

Although the municipality maintained sound operational practices, such as consistent patching, effective access management, and responsive IT operations, it had never formally adopted a cybersecurity framework, such as the NIST Cybersecurity Framework (CSF) or the CIS Critical Security Controls.

Without that foundation, a traditional compliance audit would measure the organization against controls it had not formally implemented or documented. That approach risked producing a discouraging report focused primarily on deficiencies rather than operational strengths, potentially undermining the IT team's credibility and creating misalignment between leadership expectations and on-the-ground reality.

The challenge was clear: How do you accurately assess cybersecurity posture when no formal framework has been adopted?

JANUS Approach

Drawing on decades of **cybersecurity consulting and IT risk assessment** experience across public and private sectors, JANUS recommended a different entry point: a **cybersecurity maturity assessment** using the Department of Homeland Security's **Cyber Resilience Review (CRR)** model.

This approach allowed the municipality to:

- Evaluate how well existing practices were working, even if informally documented
- Identify operational strengths and measurable improvement opportunities.
- Begin aligning security governance with the NIST CSF to lay a foundation for future compliance audits.

As a trusted partner rather than a transactional vendor, JANUS guided the client through structured workshops with IT staff and departmental stakeholders to assess controls, document operational processes, and benchmark maturity levels against recognized industry standards. **The goal was clarity, not compliance theater; a realistic picture of where the organization stood and a pragmatic roadmap for improvement.**

Solution and Implementation

JANUS conducted a comprehensive maturity assessment covering five core functions: Identify, Protect, Detect, Respond, and Recover. The assessment included:

- **Evaluating current practices** in patch management, identity and access controls, and incident response capabilities
- **Mapping informal procedures** to recognized cybersecurity controls within the NIST CSF and CIS frameworks
- **Documenting existing governance structures** and policy frameworks to establish traceability and accountability
- **Facilitating cross-functional workshops** to validate findings and ensure alignment across IT and executive leadership

© 2026 JANUS Associates, Inc. All rights reserved.
This case study is protected by applicable copyright laws, and no part may be reproduced, distributed, or transmitted in any form without prior written permission from JANUS Associates, Inc., except for brief, properly attributed quotations used in non-commercial contexts.

Rather than issuing a binary pass/fail audit report, JANUS delivered a comprehensive cybersecurity maturity profile that recognized partial implementations, pragmatic security measures already in place, and opportunities for structured improvement.

Interactive debrief sessions helped leadership translate technical findings into actionable business priorities, with clear recommendations tied to risk reduction and operational resilience.

Results and Impact

The maturity assessment provided clear, balanced visibility into the municipality's cybersecurity posture and created momentum for strategic improvement. Key outcomes included:

Improved Executive Understanding

Leadership gained visibility into cybersecurity strengths and vulnerabilities through alignment with required frameworks, enabling data-driven decision-making.

Enhanced Governance Maturity

Formal documentation initiatives were launched across departments, establishing accountability structures and preparing the organization for future compliance audits.

Risk-Based Prioritization

The municipality shifted from reactive IT management to a structured approach, prioritizing investments based on risk exposure rather than anecdotal concerns or vendor recommendations.

Increased Leadership Buy-In

Conversations shifted from *"How bad is it?"* to *"What should we do next?"*, creating alignment between IT operations and organizational leadership around a shared cybersecurity strategy.

Foundation for Compliance Readiness

Within days after receiving the report, the organization began formalizing controls and preparing for a structured NIST-based compliance audit, supported by JANUS's ongoing cyber security services and cyber risk strategy advisory.

Why JANUS Associates

JANUS Associates brings over 37 years of multi-sector expertise in IT risk assessment, vulnerability management, penetration testing, and compliance audits for both public and private organizations. Our consultants apply industry-recognized frameworks such as NIST CSF, CIS Controls, ISO 27001, and HIPAA security rules to deliver measurable improvements in resilience, cyber security and data privacy.

For this municipality, JANUS's pragmatic, partnership-driven approach transformed an audit request into a structured pathway toward program maturity and long-term security governance.

We meet entities where they are and help them get where they need to be.

Municipal and public sector leaders face the same accountability pressures as large enterprises, without the same resources. A cybersecurity maturity assessment can provide the clarity and momentum needed to strengthen governance, demonstrate due diligence, and prepare for formal compliance audits.

Contact JANUS Associates to schedule a cybersecurity risk assessment or a compliance readiness review, and to establish a strategic roadmap toward a more resilient security posture.

© 2026 JANUS Associates, Inc. All rights reserved.
This case study is protected by applicable copyright laws, and no part may be reproduced, distributed, or transmitted in any form without prior written permission from JANUS Associates, Inc., except for brief, properly attributed quotations used in non-commercial contexts.