Wolters Kluwer TeamMate

How SABIC modernized cybersecurity governance with TeamMate

A global manufacturer facing modern cybersecurity realities

SABIC is a major international chemical and materials company that operates across numerous sectors—from petrochemicals to engineered thermoplastics—and manages a substantial footprint of manufacturing sites across the United States, Mexico, and Brazil. Within this landscape, cybersecurity is no longer a back-office technical function; it is a strategic capability essential to protecting the operational technologies (OT) that drive production, safety, and innovation.

For Aaron Renschler, an OT Cybersecurity Engineer embedded within SABIC's Engineered Thermoplastics (ETP-W) business unit, managing this complexity had long been a challenge. The team's responsibility spans everything from safeguarding PLCs and HMI displays to securing precursor chemical production systems that supply industries including automotive, aerospace, and electronics. Yet the cybersecurity team itself is surprisingly lean—with six engineers supporting all major sites across the Americas.

Despite their deep technical expertise, Aaron and his peers were faced with a problem that affects many specialized engineering teams: the burden of documentation, governance, and follow-up. The work itself was always completed—but capturing, tracking, standardizing, and validating that work across a vast landscape of controls was always a difficult task.

That is, until they adopted TeamMate.

The challenge: A small team managing a big risk surface

As manufacturing systems grew more interconnected and regulatory expectations intensified, SABIC's cybersecurity needs became increasingly documentation-heavy. The team faced:

- **A massive and diverse OT asset portfolio:** OT cybersecurity isn't limited to servers and PCs. Each plant consists of layers of specialized industrial hardware—logic controllers, operator terminals, proprietary devices, and more. Managing risk across this environment requires a structured, repeatable process.
- **A small team stretched across the continent:** With a team of six people covering the Americas, each engineer is responsible not only for day-to-day protection, but also for internal validations, control reviews, and audits.
- **A lack of consistent documentation:** Prior to adopting TeamMate, Aaron's team relied on a patchwork of Excel spreadsheets, Word documents, shared drives with inconsistent folder names, and the occasional Power BI dashboards. Over time, evidence became difficult to manage, folder permissions broke, and critical documentation became a task of finding "a needle in a haystack."
- **Extreme manual effort for even basic reporting:** Pulling metrics or reviewing past assessments could consume hours of detective work. Because every plant, engineer, and assessment used slightly different naming conventions, categorization, or document storage, compiling insights across sites was daunting.
- **Corporate oversight with limited visibility:** Many reviews required input from a variety of teams, including in Saudi Arabia. Without a centralized repository, Aaron's team had no way to confirm whether reviewers saw requests, read evidence, or provided timely feedback.

For a team responsible for protecting high-stakes industrial processes, administrative duties wasn't just inconvenient—it limited the organization's ability to demonstrate maturity, plan strategically, and justify resources.

The turning point: Choosing a centralized platform

When SABIC began seeking a solution, Aaron had already visualized what an ideal cybersecurity compliance framework might look like. He had spent years refining Excel-based models, taxonomies, and linkages—painful to maintain, but conceptually sound. By the time implementation discussions began, he already knew the structure he needed. What he lacked was a tool capable of bringing it to life.

TeamMate provided exactly that, including:

- A central repository for assessments, work papers, issues, evidence, and historical results.
- A customizable taxonomy that could align with SABIC's cybersecurity standards such as NIST, ISA/IEC 62443 and C2M2.
- Self-assessment capabilities that empowered auditees and stakeholders outside cybersecurity.
- Observer roles that allowed corporate entities to review without granting excessive access.
- Automated reporting and daily insights, eliminating the need for lengthy status meetings.

For Aaron and his team, this was more than a software implementation. It was a necessary reimagining of their entire governance approach.

A new foundation: Standardization and structure through TeamMate

One of the "game-changing" features for SABIC was TeamMate's ability to bring consistency to an inherently complex environment. Before TeamMate, every engineer might label a control, categorize a risk, or store evidence slightly differently. Now, TeamMate provides greater:

- Standardized naming conventions
- Uniform document structures
- Shared objectives, controls, and evidence fields
- Consistent 'Yes/No' or scoring responses
- Repeatable assessments, regardless of who performs them

Adding to the complexity of Aaron's responsibilities, the cybersecurity domain includes over 100 distinct controls, each mapped to multiple frameworks. TeamMate allows these controls to be structured and cross-referenced precisely, enabling Aaron's team to perform analysis they simply couldn't do before.

When corporate auditors or regulators asked, "How does the business perform in this particular cybersecurity domain?" the team was challenged to provide a timely and appropriate answer. With TeamMate, Aaron is now able to instantly view things like control history, compliance status by site, past assessment frequency, evidence trails, and trends over time.

These new capabilities transformed SABIC's ability to justify resources, when and where needed. And in a manufacturing environment where cybersecurity competes with concerns like corroding pipes or mechanical failure, clearly articulated risk supported by data is essential.

Streamlined coordination

International collaboration was previously one of the biggest pain points for the SABIC team. Corporate reviewers often needed to validate findings, but communication could be inconsistent and difficult to trace.

TeamMate was able to change that dynamic by providing:

- **Observer roles** that allow corporate teams to see only what they need—objectives, comments, and approvals—without granting full access.
- **Audit trails** that allow engineers to confirm exactly who has reviewed which piece of documentation.
- **Automated emails and embedded links** that prevent requests from disappearing into inboxes.

For the first time, the cybersecurity team at SABIC could track a variety of follow-up actions across the lifecycle of an assessment, without relying on email threads or shared drive folders.

Empowering auditees and increasing engagement

An early achievement from the team involved implementing self-assessments and issue tracking. While some organizations adopt these capabilities later, SABIC expressed an interest to embrace them immediately.

Since taking steps to implement self-assessments and issue tracking:

- Auditees log in directly to complete self-assessments
- Recommendations and issues flow seamlessly to those responsible
- Progress can be monitored in real time
- Follow-ups that required hours of meetings are handled automatically

This shift has significantly reduced the overall administrative burden and strengthened ownership at the plant level.

Unlocking new capacity: Doing more with the same team

Perhaps the most profound impact of TeamMate was how it enabled the SABIC team to expand their work without expanding headcount. Before TeamMate, it was a struggle to document even the most essential activities while balancing daily responsibilities. Now they can quickly and seamlessly:

- Build repeatable forms and templates
- Launch quarterly control validations (e.g., access reviews, firewall checks)
- Perform targeted control assessments with minimal prep
- Automate reporting and dashboarding
- Attach all evidence directly within the platform

Aaron describes it simply: “Our ability to expand beyond just the big audits happened very quickly. Within a few sessions, I realized I could use TeamMate for far more than I expected.”

A mature, traceable audit trail

A major differentiator for TeamMate is its ability to maintain historical insights—a complete audit trail of assessments, evidence, decisions, and outcomes. For cybersecurity especially, maturity matters. Auditors want to know if the controls are functioning consistently, is this a one-off improvement or a sustained practice, and can the team demonstrate a pattern of behavior, not just recent activity?

Thanks to TeamMate, evidence no longer disappears, and controls have historical continuity across sites and years. Additionally, SABIC is now capable of demonstrating that validations have been performed repeatedly—not just in preparation for an audit. This has greatly improved the quality of the team’s audit posture and strengthened the credibility of the cybersecurity program as a whole.

Implementing TeamMate: The importance of having a vision

For Aaron, one of the reasons the implementation succeeded so quickly is that he knew what he wanted before he began. Years of wrestling with Excel had forced him to think deeply about things like domain structures, control categorization, linkages between questions and objectives, and evidence types and reporting expectations, to name a few.

When TeamMate was first implemented, he could focus on learning the application—rather than designing a methodology from scratch. He dedicated time each week during implementation simply experimenting, designing assessments, reviewing reporting structures, and training other members of his team. That investment paid off, and the system now aligns directly to SABIC's cybersecurity methodology, rather than forcing the team to compromise.

Aaron's advice to others considering automation with TeamMate is clear: "If you want to maximize the benefits of TeamMate, you have to spend time building, practicing, and educating your team. It's not complicated, but it rewards the effort you put into it."

The outcome: A more confident, efficient, and visible cybersecurity program

SABIC's journey from scattered spreadsheets to centralized, structured governance exemplifies the power of aligning the right tools with a team's strategic vision. For a small cybersecurity team within a massive industrial enterprise, TeamMate became far more than a system for audits—it became the backbone of their governance, risk, and compliance strategy through:

1. **Time savings on administrative work:** A three-week audit previously required daily two-hour review meetings. With TeamMate's automated reporting and Team Insights, those meetings practically vanished.

2. **Stronger collaboration with global partners:** Corporate review cycles that once disappeared into inboxes are now transparent, traceable, and neatly integrated into workflows.

3. **Greater maturity and credibility:** Historical evidence and consistent documentation provide a clear, defensible audit trail.

4. **Increased operational capacity without staffing increases:** The six-person team can now run quarterly reviews, perform targeted validations, and expand compliance activities across all major sites.

5. **Empowered auditees and streamlined issue resolution:** Self-assessment and issue tracking capabilities eliminate the reliance on spreadsheets and ad-hoc communication.

6. **A scalable foundation for analytics:** As SABIC continues to accumulate structured data, advanced analytics will become increasingly powerful.

The transformation of the SABIC team is evident and has resulted in more assessments with less effort, better insights with less manual work, stronger collaboration with fewer communication gaps, and greater maturity with clearer documentation. Most importantly, TeamMate allowed SABIC's cybersecurity team to focus on what truly matters—securing the critical systems that power global manufacturing.

Contact information

Americas
4221 W Boy Scout Blvd #500
Tampa, FL 33607
U.S.A.

303 W Pender St
Vancouver, BC V6B 1T3

Europe, Middle East, and Africa
8th Floor
30 Churchill Place
Canary Wharf
London
E14 5RE
United Kingdom

Asia Pacific
5 Shenton Way
#20-01/03 UIC Building
Singapore 068808

Please visit **tm.wolterskluwer.com**
for more information.