

Defining the Pool's Role in Member Cyber Resilience

*Support, expectations, and where member
responsibility begins*



Table of contents

■ Introduction	03
■ How much does the pool need to know?	04
■ What happens after the pool finds something?	06
■ What should the pool provide—and what should it expect in return?	08
■ How does the pool know whether its approach is working?	10
■ Defining the role in practice	12
■ Sources & notes	14

Introduction

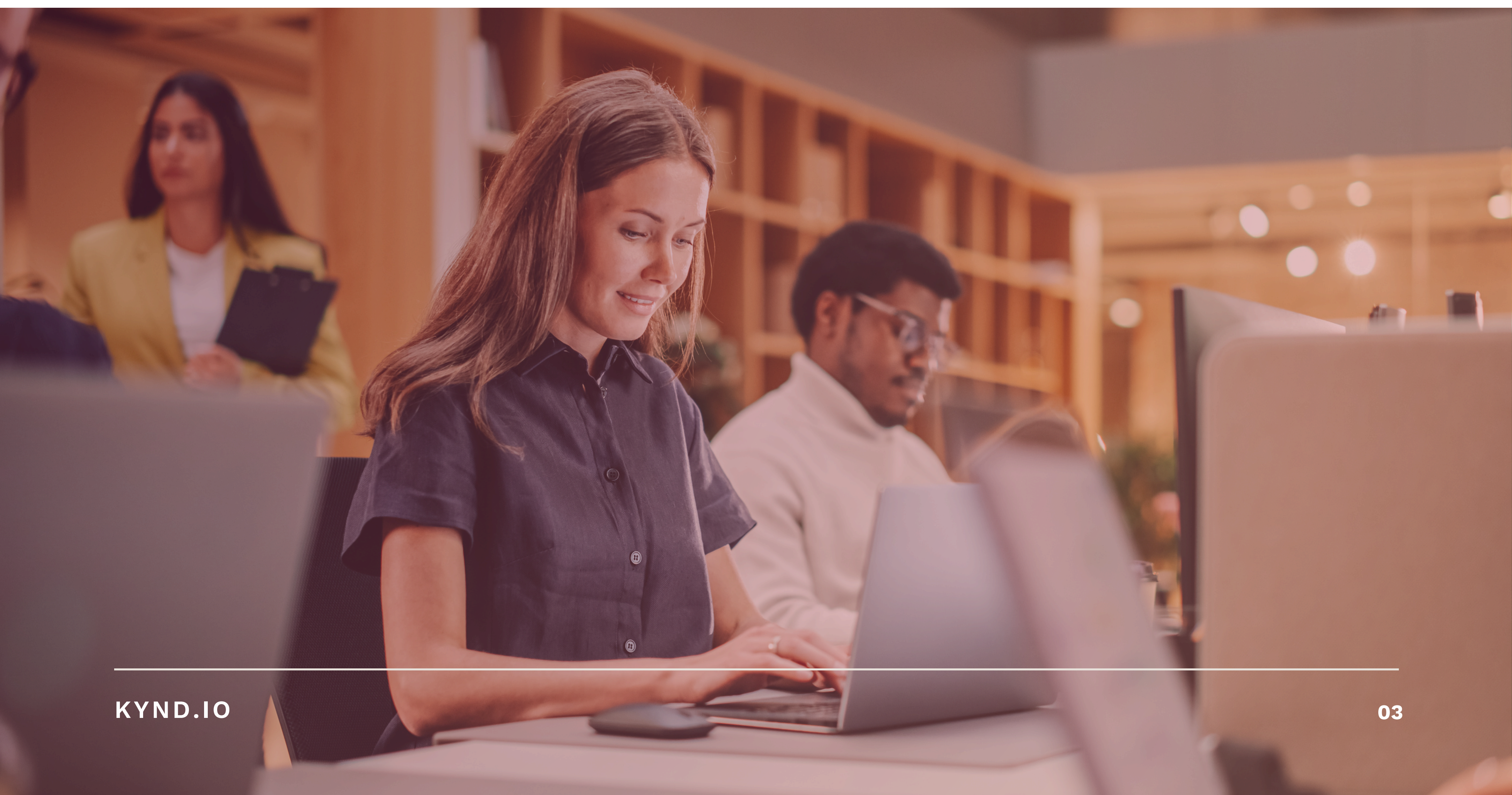
For public entity pools, understanding cyber risk across the membership isn't simple.

Members have different levels of staffing, resources and technical maturity, while the information available to the pool often comes from different places—applications, claims, renewal conversations and members themselves. Building a clear, consistent picture takes work.

But visibility is only the beginning. Once a pool can see where risk sits, a different set of questions emerges: Where should it focus? How far should it go in helping a member act? What should it reasonably expect from members in return? And

how will it know whether its approach is working?

Our conversations with pools over the past year suggest there is no single answer. But they do point to several common themes in how pools are beginning to define their role.



How much does the pool need to know?

Better visibility doesn't necessarily come from asking members for more.

Pools need enough information to understand where risk sits across the membership, but members vary significantly in what they can realistically provide.

The challenge is building a clearer picture without simply adding to the burden.

Debbie Yokota, CEO of the Special District Risk Management Authority (SDRMA), describes why that matters at scale. With more than 600 public agency members whose needs and capabilities vary widely, understanding systemic cyber risk across the pool—and identifying where attention is needed most—has become increasingly important.¹

Building that picture can be difficult because the relevant information often sits across different parts of a member organization.

At Schools Insurance Group (SIG), district technology teams were focused on education and instruction rather than insurance or underwriting. The districts themselves also operated across different platforms, vendors and approaches. As Kris Packwood, Director of Risk Services put it, "everyone was rowing their own way."²

“

Cyber is one of those areas where the landscape is changing quickly, where members' needs and capabilities can vary widely, and where understanding systemic cyber risk across the pool is becoming increasingly important.

Debbie Yokota
CEO, SDRMA

“

Everyone was rowing their own way. What we needed was a way to get everyone into the same boat, rowing in the same direction.

Kris Packwood
Director of Risk Services, SIG

At the South Carolina School Boards Insurance Trust (SCSBIT), Director of Insurance Services Lyde Graham kept the annual process streamlined across more than 50 districts, and judged any new approach by whether it would add to an already stretched IT function. "We needed something portable, not tied to the carrier," he said, "because anything new is already a heavy lift for our districts."³



KYND gives us clarity to focus resources where they matter most, and it helps our members quickly discern opportunities to strengthen their postures. It also provides a one-portable solution that isn't tied to what a specific carrier may offer, which is critical when competition or program changes lead to a carrier shift.

Lyde Graham

Director of Insurance Services, SCSBIT

Brennan Hickok, Director of Operations at the Alaska Public Risk Alliance (APRA), sees the capacity challenge from another angle: some members contract out IT; at others, one employee carries several roles alongside it. Cyber can compete for limited time and budget against water, roads, fuel and other essential needs.⁴

That also creates a scale problem for the pool itself.

A pool with hundreds of members cannot necessarily begin by interviewing every organization individually. Applications, renewal information, claims history, observable external exposure and existing member or managed-service-provider evidence may already establish a meaningful part of the baseline.

Member input can then be focused on what the pool still needs to know. The objective is not perfect information. It is enough reliable information to decide where attention should go first.

What happens after the pool finds something?

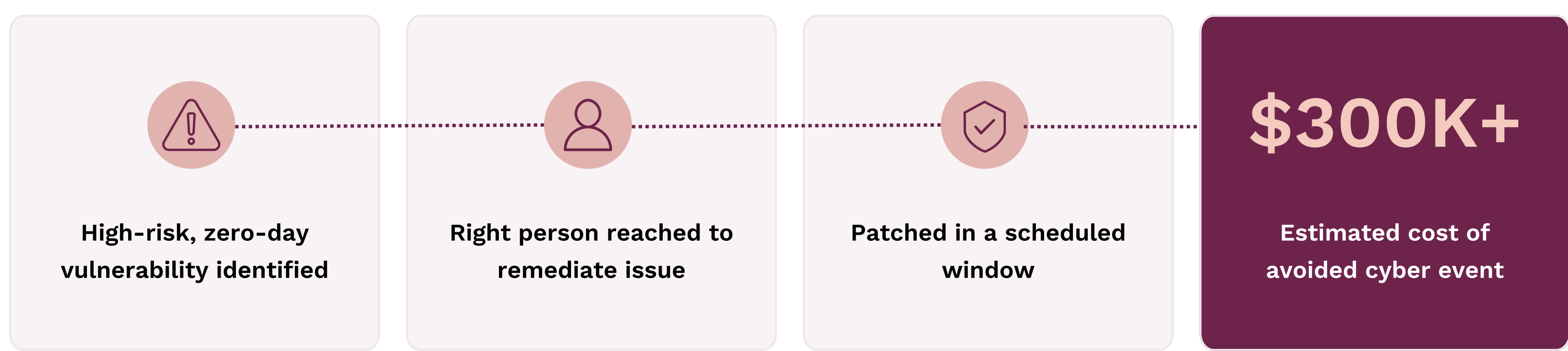
Identifying risk is only part of the job. The next challenge is helping move an issue from visibility to action.

Pools typically aren't the ones implementing the technical fix. But their relationships with members can put them in a valuable position between identifying an issue and seeing it addressed: getting the information to the right person, helping establish what needs to happen next and staying engaged as the member acts.

SCSBIT saw this firsthand when a high-risk, zero-day vulnerability was identified at one member district. Because the exposure could be tied to a specific district and system, Graham knew where attention was needed and reached the district's IT director directly.³

Remediation was completed during a scheduled weekend window, before the vulnerability could be exploited. There was no disruption to instruction and no operational downtime. SCSBIT estimated that a costly cyber event—potentially exceeding \$300,000 in response, legal and recovery costs—was avoided.³

"If that alert hadn't come through," Graham said, "it wouldn't have been a matter of if something happened, but when."³



What stands out in the sequence isn't only the alert. SCSBIT could tell which member was exposed and to what, get to the person who could act, and see the fix land in a window that didn't cost instructional time.

That handoff—from a pool's finding to a member's action—is where Eric Swagerty, Member Relations Representative at Enduris, puts the emphasis: understanding what the member needs, connecting them directly with the right resource or person, providing context and staying engaged rather than simply passing along information. For Enduris, that role relies heavily on the relationships the pool already has with its members.⁵

The pool does not have to become the cybersecurity provider. It can instead act as a guide, connector and matchmaker—with follow-through.

“

If that alert hadn't come through, it wouldn't have been a matter of if something happened, but when.

Lyde Graham

Director of Insurance Services,
SCSBIT



What should the pool provide—and what should it expect in return?

Support and expectations don't have to sit on opposite sides of the equation.

Across the approaches we heard, the two often work together. Support can make progress more achievable, particularly for members with limited resources. Clear expectations can help members understand where to focus and what responsible participation in a shared-risk environment looks like.

SIG's Cyber Safety Credit Program offers one approach. Cyber had previously been folded into a broader safety credit structure alongside property, liability and workers' compensation; separating it reflected a view that cyber warranted its own framework. Districts earn credits for participating in cyber sessions, making progress on foundational controls such as multi-factor authentication, engaging with cyber insights and completing applications on time.²

"We wanted to empower members, not penalize them," said Executive Director Dr. Kelli Hanson. "The credits give districts a roadmap. They can see what good looks like, prioritize over time, and still move at a pace that fits their reality."²

That last point matters. A control that a well-resourced district can implement in weeks may take a smaller district considerably longer. The credits are designed to focus effort, helping districts prioritize where time and investment go rather than expecting every member to move at the same pace.²

“

We wanted to empower members, not penalize them. The credits give districts a roadmap. They can see what good looks like, prioritize over time, and still move at a pace that fits their reality.

Dr. Kelli Hanson
Executive Director, SIG

Enduris pairs support with clearer expectations, including a mechanism that waives a portion of a member's cyber claim copay where expectations are met. Swagerty frames the underlying principle in community terms: pool members share risk, and with that comes a shared interest in each member taking reasonable steps to manage it.⁵

Published material from other public entity pools shows different ways those expectations can take shape. One pool links what a member pays toward a cyber claim to the security standards it has met; another structures member retention and coinsurance around a defined set of cyber control elements.⁶

The mechanisms differ, and none removes the realities on either side. Resistance to controls that depend heavily on changes in human behavior, and the cost of supporting them across a large membership, can still slow progress.⁶

What the approaches have in common is not a particular incentive or requirement. It is a recognition that the pool's role can include both helping members move forward and becoming clearer about what it expects in return. Where that balance sits will depend on the pool and its membership.



How does the pool know whether its approach is working?

Progress won't look the same across every member, but pools still need a way to see whether risk is moving over time.

Assessments completed, reports issued and sessions delivered show that a cyber program is active. They do not necessarily show that the membership is resilient.

A consistent baseline helps pools track where controls are strengthening and gaps persist. For newer programs, progress may begin with participation and clearer ownership. As programs mature, pools can look more closely at changes in specific controls and exposures.

Tracking these indicators over time turns a snapshot of risk into evidence of progress, helping pools understand what has changed and where to focus next.



The important thing for us isn’t simply seeing the risk—it’s seeing whether we’re making progress. We can demonstrate meaningful improvement across the membership, understand where gaps remain and focus our resources where they’re needed most, without the pool having to become a cyber operations team.

Deborah Callahan
CEO, WSRMP

One pool's view over three years

Across three years of continuous monitoring, member-reported controls across the Washington Schools Risk Management Pool (WSRMP) membership moved materially:

Continuity & Recovery Planning

8% → 69%



Multi-Factor Authentication for Remote Access

35% → 87%



July 2023–June 2026. One pool's experience. Controls are member-reported.⁷

That evidence can also strengthen the broader insurance conversation. Simon Meech, Cyber Growth Leader at BMS, notes that underwriters continue to differentiate based on the quality of the risk, making evidence of member progress increasingly valuable: "Increasingly, the difference comes down to evidence, not intent."⁸

For the pool itself, however, the more immediate value is knowing where risk has improved, where gaps remain and where additional attention may be needed. That creates a stronger basis for deciding what comes next.



For pools, being able to demonstrate what members are doing to improve their cyber posture—and provide evidence of that progress—can make a meaningful difference in the renewal conversation. Increasingly, the difference comes down to evidence, not intent.

Simon Meech
Cyber Growth Leader, BMS

A possible next step: matching support to members’ starting points

As pools build a more consistent view of member risk, they may be able to distinguish members who need priority support to establish foundational controls, those developing their approach who have made a start but still have important gaps to address, and stronger members focused on sustaining progress and resolving remaining exposures.

● Priority Members

Foundational controls are missing or unverified, significant exposures need attention, or limited engagement is hindering progress.

Pool focus: Set minimum expectations, provide direct support and closer follow-up, and escalate where appropriate.

● Developing Members

Some foundational controls are established, but important gaps remain or evidence of implementation is still incomplete.

Pool focus: Agree on achievable next steps, connect members with targeted support and follow up on remaining gaps.

● Stronger Members

Foundational controls are supported by evidence, significant known exposures are limited, and the member is actively engaged.

Pool focus: Sustain progress, strengthen remaining areas and encourage members to share experience with peers.

These are not fixed labels. The value is in matching support and expectations to each member’s needs—and seeing whether members move forward over time.

Defining the role in practice

There is no single model for the pool's role in member cyber resilience. Membership, resources, coverage environment and program maturity all shape what is realistic. But the experiences shared by pools point to several principles worth carrying forward.

Build visibility without simply adding burden.

Pools need a reliable view across the membership, but more questions don't automatically create more insight. Consider what members can realistically provide, what information already exists and where another source of visibility may be needed.

Turn visibility into priorities.

Bring together what members report, what can be observed externally and what can be verified. This can help the pool see members at different starting points: some need help establishing foundational controls, while others need targeted attention on a few remaining gaps. The point is to make the next step clearer for each member.

Match the intervention to the member and the problem.

Not every finding calls for the same response. Some warrant shared guidelines; others call for direct outreach, a connection to specialist support or closer follow-up. Consider the member's capacity and what it can realistically do next.

Pair support with clear expectations.

Members may need education, resources, prioritization and time to make progress. Clear expectations can sit alongside that support, giving members a better understanding of where to focus and what the pool expects as part of a shared-risk community.

Measure movement, not just activity.

Progress will look different depending on where members and programs begin. A consistent baseline gives pools a way to see whether controls and exposures are changing over time—and then use that evidence to guide investment, intervention, leadership decisions and the insurance conversation.

The objective is to help members make progress from different starting points, while giving the pool a clearer view of where risk remains and where to focus next.

Those principles still leave important choices for each pool to make. How much of the member journey should the pool help facilitate? Where should support give way to member ownership? What incentives or consequences are appropriate? And as expectations evolve, how will the pool know whether its approach is producing meaningful progress?

The line will look different for every pool. What matters is defining it deliberately, rather than allowing it to be defined only when a member incident forces the question.

Where does your pool go from here?

KYND works with public entity risk pools to build clearer visibility across their membership, focus support where it's needed most and measure how cyber risk changes over time.

If you're thinking through what that could look like for your pool, we'd welcome the conversation.

Learn more at kynd.io or contact Ben Duffy at bduffy@kynd.io

Sources & notes

1. Debbie Yokota, CEO, Special District Risk Management Authority. Quoted in KYND's Cyber Drop newsletter, July 23, 2026.
2. "From Cyber Activity to Member Movement—How One Pool Built a More Defensible Cyber Program," KYND, May 28, 2026. support.kynd.io/public-entity-blog/from-cyber-activity-to-member-movement-how-one-pool-built-a-more-defensible-cyber-program
3. "Inside the Cyber Risk Playbook: How One School Risk Pool Avoided a Costly Cyber Incident," KYND, April 8, 2026. support.kynd.io/public-entity-blog/inside-the-cyber-risk-playbook-how-one-school-risk-pool-avoided-a-costly-cyber-incident
4. Brennan Hickok, Director of Operations, Alaska Public Risk Alliance. From "Strengthening Cyber Resilience Across Your Membership," AGRiP Staff Institute, Oct. 6, 2026.
5. Eric Swagerty, Member Relations Representative, Enduris. From "Strengthening Cyber Resilience Across Your Membership," AGRiP Staff Institute, Oct. 6, 2026.
6. "Cyber Coverage Creativity in a Hard Market," Risk Program Administrators, 2022. rpadmin.com/media/2079/rpa_cyber-coverage-creativity-in-a-hard-market-9-22.pdf
7. Washington Schools Risk Management Pool. KYND data, July 2023–June 2026.
8. Simon Meech, Cyber Growth Leader, BMS. Quoted in KYND's Cyber Drop newsletter, Aug. 27, 2026.