BACKSTOP Alignment with ISACA State of Cybersecurity 2025

Executive Summary

The ISACA State of Cybersecurity 2025 report highlights chronic resource constraints, inconsistent cyber risk assessments, and challenges in Board-level communication.

BACKSTOP aligns strongly with these needs by providing structure, prioritization, and defensible reporting here's how:

1. Cyber Risk Assessments

ISACA highlights that many organizations perform cyberrisk assessments infrequently or not at all due to time, staffing, and reporting constraints. BACKSTOP enables repeatable, lightweight risk assessments with centralized scoring and automated reporting.

2. Board Oversight and Cybersecurity Prioritization

Only 56% of Boards adequately prioritize cybersecurity. BACKSTOP supports Board-ready dashboards that translate technical risk into business-relevant insights, improving oversight and alignment.

3. Resource Constraints and Understaffing

With over half of cybersecurity teams understaffed, BACKSTOP acts as a force multiplier by embedding governance and structure into a single platform, reducing reliance on scarce expertise.

4. Consolidation and Reporting

ISACA identifies consolidation and reporting as major pain points. BACKSTOP provides a single system of record for risks, controls, frameworks, and remediation activities.

5. Framework Alignment

BACKSTOP supports multi-framework mapping (e.g., NIST, ISO, SOC) without creating unnecessary compliance overhead, allowing risk to drive priorities.

6. Confidence in Cybersecurity Posture

Only 41% of respondents are confident in their ability to detect and respond to threats. BACKSTOP improves governance confidence by demonstrating known risks, control status, and active remediation.

BACKSTOP does not replace SOC, MDR, EDR, or real-time threat detection tools. Its value lies in governance, not operational security tooling.