TLP:AMBER

CISO EXECUTIVE REPORT

ACME FINANCIAL SERVICES

March 31, 2026

ACME FINANCIAL SERVICES 03/31/2026

TLP AMBER CISO
EXECUTIVE REPORT

This report corresponds to March 2026 and it is directed to Director or VP of IT, Cyber Security, Cyber Security Compliance or equivalent. The information is delivered following the GLESEC`s Seven Elements Cyber Security Model (7eCSM TM), these elements are: Risk, Vulnerabilities, Threats, Assets, Compliance, Cyber Security Validation and Access

ABOUT THIS REPORT

The purpose of this document is to report on the “state” of security for your organization. It must be noted that GLESEC bases its information analysis on the services under contract. The information generated by these services is then aggregated, correlated and analyzed.

RISK

Actual Risk

31%

During March, ACME recorded an Actual Risk level of 31%, reflecting a continued increase in overall exposure across the assessed environment. This result indicates that multiple conditions and findings remained active during the month, contributing to a broader risk surface. While this value does not necessarily imply immediate compromise, it does highlight the importance of maintaining continuous monitoring and prioritizing mitigation efforts to prevent further escalation.

Accepted Risk

5%

During March, the Accepted Risk level stood at 5%, indicating that a limited portion of the identified exposure has been acknowledged and assumed under controlled conditions. This suggests that ACME continues to maintain a cautious and structured approach to risk tolerance, allowing only a small percentage of exposure to remain accepted based on operational or business considerations.

Confidence

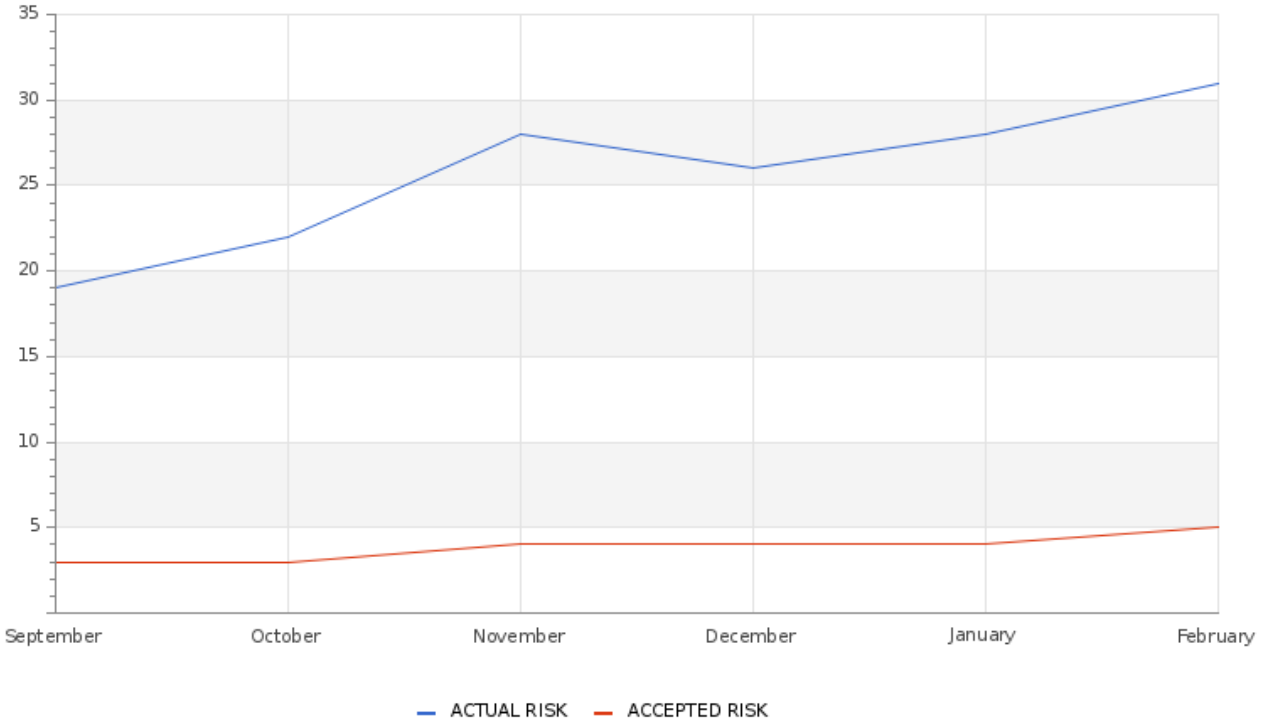
Medium

For March, the confidence level remained Medium, indicating that there is sufficient information available to support a reasonable interpretation of the organization’s current risk landscape. At the same time, additional context, validation, or broader data correlation may further strengthen future assessments and support more informed strategic decisions.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

ACME FINANCIAL SERVICES 03/31/2026

Accepted & Actual Risk



During the last six months leading into March, ACME's overall risk posture showed a sustained upward trend, with Actual Risk increasing from 19% in September to 31% in February, maintaining this elevated level into March. Although slight fluctuations were observed during the period, the overall pattern reflects growing exposure across the environment. Accepted Risk remained comparatively low, increasing gradually from 3% to 5%, which suggests that risk tolerance continues to be limited and controlled. This trend indicates that, while the organization maintains a cautious posture regarding accepted exposure, the increase in actual risk observed up to and during March reinforces the need for continued monitoring and prioritized mitigation efforts.

VULNERABILITY

THREATS

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
Change in Systems Performance	19
High Persistency Detection	2
BAS Web Security	24
Threat Intelligence Detection	10
Change in Systems Availability	24
EDR Alerts	3
Internal user deleted or moved a SoftwareMine	61
BAS WAF	2
Notable Event Alert: Risk of Threats and Vulnerability Correlation. Alert	60
Change in Internal High or Critical Vulnerabilities for IT, IoT and OT	1
Change in External High or Critical Vulnerabilities	60
Non Baselined Discovered System	8

During March, ACME recorded a significant number of notable operational and security-related events across multiple monitoring and detection categories. The most recurrent activity was associated with Internal user deleted or moved a SoftwareMine with 61 events, followed closely by Notable Event Alert: Risk of Threats and Vulnerability Correlation and Change in External High or Critical Vulnerabilities, both with 60 events each. In addition, BAS Web Security and Change in Systems Availability registered 24 events respectively, while Change in Systems Performance accounted for 19 events.

Other categories showed lower but still relevant activity, including Threat Intelligence Detection with 10 events, Non Baselined Discovered System with 8 events, EDR Alerts with 3 events, and both High Persistency Detection and BAS WAF with 2 events each. Change in Internal High or Critical Vulnerabilities for IT, IoT and OT registered 1 event during the month.

Overall, the volume and distribution of events observed in March indicate an active monitoring environment with visibility across performance, availability, vulnerability exposure, user activity, and threat detection. The concentration of events related to vulnerability changes, risk correlation, and file activity suggests that continued attention should be placed on exposure management, asset control, and the validation of potentially impactful operational changes.

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TLP:AMBER

CISO EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500