



# Cyber Insurance Risk & Readiness

ACME Group

Report Generated: 12/08/2025

# Overview

We have conducted a comprehensive 360-degree risk assessment of your company and the essential cyber defenses within your supply chain. Through an in-depth analysis of your external attack surface, internal cyber controls, and financial risk impact, we can accurately pinpoint your cybersecurity exposure.

The aim of this report is to provide valuable insights into your company's cybersecurity posture and to support your company's investment strategy in cyber defenses.



## 360 Risk Assessment

The 360-degree risk assessment involves three core cyber elements tailored to assess your company and your critical supply chain: Attack Surface, Compliance Risk, and Financial Risk Quantification. The integration of these three evaluations provides a comprehensive 360-degree understanding of your cyber exposure, enabling strategic planning and effective mitigation of potential cyber-attacks.

### Attack Surface Management

Company & Supply Chain  
websites and web-apps .



### Compliance Risk Assessment

Company & Supply Chain  
Cyber Control Assessment.

### Financial Risk Quantification

Company  
Financial Exposure

This report combines the observation of your company and supply chain cybersecurity defences, delivering industry-standard insights.

Cyber Rating – Compliance Risk - Financial Exposure - Remediation Plans

## Attack Surface, Compliance and Risk Quantification



**Attack Surface Management (ASM).** ASM is a non-intrusive cybersecurity assessment of a company's internet-facing web servers - web applications, websites, and email systems.

This assessment examines the security settings and potential vulnerabilities within these systems, yielding a comprehensive cybersecurity score and remediation recommendation. Through the implementation of strong cyber controls, the organization can achieve a praiseworthy ASM rating, thereby reducing the likelihood of potential cyber-attacks.

**Compliance Risk Management (CRM).** CRM ratings reflect the organization's adherence to regulatory requirements and industry-standard controls and policies.

Encompassing aspects such as data protection, privacy regulations, and security frameworks. The assessment reveals that the organization has demonstrated a high level of commitment to compliance, earning a favorable CRM rating.

**Financial Risk Quantification (FRQ).** The FRQ focuses on the organization's preparedness to handle financial losses in the event of a cybersecurity incident.

Consideration factors such as CRM, ASM ratings, and asset values are calculated to build a loss expectancy and budget requirement to mitigate cyber risks.

In Addition... not rated. We provide an observation of your company's **Threat Intelligence (TI)**. TI provides insights into emerging threats, attack vectors, and indicators of compromise. The report includes a comprehensive overview of the threat landscape relevant to the organization, enabling proactive threat detection and response. It also provides recommendations for leveraging threat intelligence to enhance the organization's overall security posture.

## Trusted Cyber Ratings

Our cybersecurity risk ratings are a reliable and trustworthy source of information for assessing the risk profile of any business.

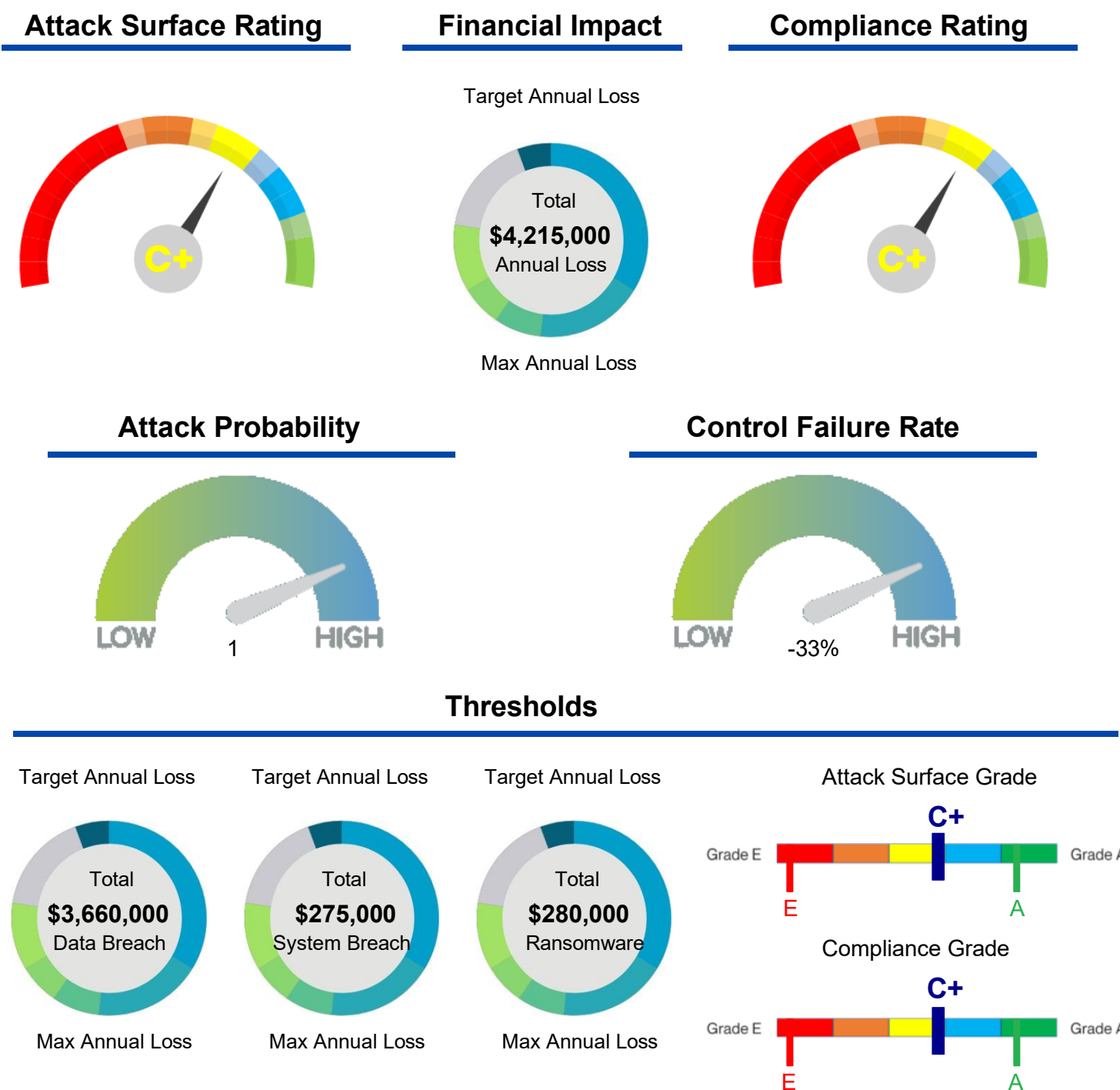
All our ratings are aligned with industry security standards, including the \*US Commerce of Trade - **Principles For Fair And Accurate Security Ratings**, \*National Institute of Standards and Technology - **NIST NVD CVE** and the \*Common Vulnerability Scoring System - **CVSS V3.0**.



# Executive Summary



This in-depth report analyzes your internet apps, data, and security controls to give a complete picture of your cybersecurity posture. It prioritizes improvement areas and offers recommendations for strengthening your defenses.

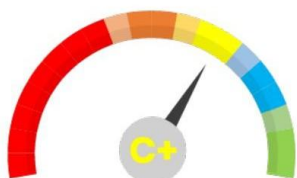




# Executive Summary Explained

Below is an explanation of how to interpret the executive summary scores and the methodology used to calculate them. Please note that the algorithms may be updated periodically to account for emerging industry profile risks and threats.

## Attack Surface



Cygenic evaluates a company's internet assets by thoroughly examining six key checkpoints with fifty-four cyber probes. The grade is assigned using an international rating system ranging from A+ to E, with an A+ indicating that the company's cybersecurity defense is at an industry-leading level.

Checkpoint	# Probes	Weight %
Email Security	6	11
Webpage Security	11	15
Data Privacy	8	14
System Compromised	5	17
System Vulnerability	8	26
Open Network Ports	16	17

Grades	Pass %	Result
A+	93-100	Leader
A+	85-92	Advanced
B+	79-84	Excellent
B	73-78	Good
C+	62-72	Average
C	55-61	Low
D+	47-54	Poor
D	40-46	V. Poor
E	0-39	Failed

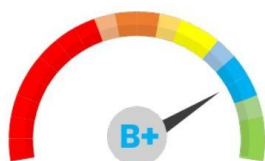
## Financial Impact



Financial Impact estimates the expected financial loss from a cyberattack. Additionally, the algorithms calculate the probability of a cyberattack, the likelihood of control failure, and the estimated insurance costs. Below are the formualars used to calculate the impact. A comprehensive report is provided in the financial quantification section of this report.

Financial Quantification	Calculation
Attack Surface Grade weighting for the probability of cyberattack	50%
Security Compliance Grade weighting for the probability of cyberattack	50%
Probability of cyber-attack calculation per year	80%=1 to 40%=3
Insurance calculation = % of event annual loss expectancy	1%
Ransomware calculation = % of total annual sales revenue	2.80%
Total Annual Loss= Data breach + System breach + Ransomware costs	ALE=
Data Breach cost per record	\$183
System Breach recovery days	10 days

## Security Compliance



Security Compliance grades stem from Cygenic's exclusive audit program, wherein each control is assessed and weighted according to the responder's input. Notably, during onboarding, companies undergo a proprietary cybersecurity survey aligned with ISO27001 standards to gauge their cyber readiness

Compliance Control Weighting	Risk Level
8	Critical
6	High
4	Medium
2	Low

Grades	Pass %	Result
A+	93-100	Leader
A+	85-92	Advanced
B+	79-84	Excellent
B	73-78	Good
C+	62-72	Average
C	55-61	Low
D+	47-54	Poor
D	40-46	V. Poor
E	0-39	Failed

Compliance Weighting		
Fully	Mostly	Partially
100%	75%	50%
Limited	Non	NA
25%	0%	Na

