RISK INDEX REPORT

Odyssey Logistics & Technology Corp

https://odysseylogistics.com

24-Jun-2026

RISK INDEX COMPANY INPUTS

Firmographics | Technologies Used | Perimeter Scanning | Threat Intelligence | Predictive Controls | Attested Controls

Risk Index

Defensibility against cyber risk is very strong. The organization demonstrates exceptional cybersecurity practices, which are highly effective in reducing risk. Controls are robust and consistently applied. Threat exposure is insignificant.

Risk Domain	Domain Index
Application Security	75 Strong
Data Protection & Privacy	82 Very Strong
Endpoint & Device Security	87 Very Strong
Human Resource Security	80 Very Strong
Identity & Access Management	82 Very Strong
Incident Response & Business Continuity	72 Strong
Network Security	83 Very Strong
Physical & Environmental Security	86 Very Strong
Threat Management	86 Very Strong
Vulnerability Management	82 Very Strong

Address
39 Old Ridgebury Road, DANBURY, CT, 6810, United States

Employee Count
2,001 - 5,000

Annual Revenue
$500M-$1B

Industry
Other Support Activities for Transportation

Description
Odyssey Logistics & Technology Corporation (OL&T) is a global logistics management service provider that internalizes the needs of its client partners in order to serve them better. The Company manages every aspect of the logistics supply chain from inbound delivery logistics through outbound shipment, handling, consolidation, deconsolidation, distribution and delivery of end products. It provides clients with cargo planning, tendering, shipment visibility and configurable event management, freight audit and payment and management reporting through its integrated transportation management system. The Company's Truck Brokerage Services offers a...

APPENDIX

Risk Index Company Inputs

Firmographics	Identifying information such as industry and domain (primary), revenue, employee range, and company age (supporting), is used to confirm company identity, define the external attack surface, and enable peer benchmarking. Firmographics Primary and supporting firmographic data is included
Technologies Used	Information about technologies deployed by the company is used to infer the presence of mapped controls. Technologies Used Technologies Used data is included and map to controls
Perimeter Scanning	Automated external scanning data identifies potential attack entry points visible to external threat actors. Perimeter Scanning Perimeter Scanning data is included
Threat Intelligence	Data from third-party intelligence providers supplies early indicators of relevant threats and attack patterns. Threat Intelligence Threat Intelligence data is included
Predictive Controls	Predictive control scoring estimates potential control effectiveness based on peer data and external signals. Predictive Controls Predictive Controls scoring is included
Attested Controls	Company-provided control attestations, ranging from a minimum of one control up to the full Core control set, contribute to an internal view of control effectiveness. Attested Controls Attested Controls responses are provided for some controls

Risk Domains

Controls are organized into Risk Domains, each representing a distinct area of cybersecurity risk management. Each domain comprises controls designed to mitigate specific risk types and threat vectors. Domain-level scoring provides targeted insight into an organization's risk posture within each area.

APPENDIX

Risk Index Methodology

ProcessUnity Risk Index is an actionable risk rating that unifies internally informed controls data with externally observed security signals to provide a comprehensive view of an organization's cyber risk posture at an overall and risk domain level.

Controls Foundation

The Risk Index is built on the Global Risk Exchange, which contains cybersecurity control data collected across hundreds of thousands of companies. The Exchange integrates multiple external data sources to gather firmographic, technographic, threat, and vulnerability information for each organization.

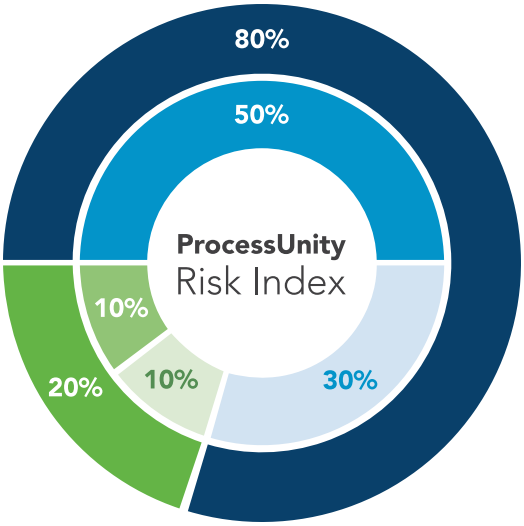
All external data is mapped to cybersecurity controls by ProcessUnity subject-matter experts. Controls are also mapped to related controls, enabling advanced relationships across the control network. These expert-driven mappings form a unique, controls-based foundation for risk assessments.

Scoring Model

The Risk Index scoring model synthesizes data from the Controls Foundation and Company Inputs to produce risk ratings at both the overall and risk domain levels. Scoring is performed across four components—security controls, vulnerability resiliency, perimeter scanning, and threat intelligence. Each component is independently calculated and weighted, then aggregated to generate a score ranging from 0 to 100, along with an associated five-band risk rating that supports interpretation of the score and assessment of the company's cyber risk defensibility.

80% Inside Out
Internally informed control data

20% Outside In
Externally observed security signals



50% Security Controls
- How well a company implements cybersecurity controls
- Evaluates the company's security maturity and control effectiveness

30% Vulnerability Resiliency
- How well a company addresses common cybersecurity weaknesses
- Indicates the company's ability to prevent and respond to security vulnerabilities

10% Perimeter Scanning
- Security vulnerabilities visible from outside the company's network
- Reveals potential attack entry points that external threats could exploit

10% Threat Intelligence
- The company's exposure to current and emerging threats
- Provides early warning of relevant threats and attack patterns

For additional risk details about a company, view their complete risk profile in your ProcessUnity platform. For more information on Exchange data and our risk methodology, please visit the ProcessUnity Exchange knowledge base Risk Index Methodology. For issues or questions, please contact our Support Email.

Disclaimer

This report was prepared exclusively for the company by ProcessUnity, Inc. It includes insights derived from any internal information provided by the company, supplemented with external data sourced by ProcessUnity and its trusted data partners, as well as benchmark information aligned to common firmographic categories. All data has been processed and transformed using computational and statistical methods designed to ensure confidentiality. The information provided in this report is confidential and intended solely for the company's limited use or to be shared with the company's clients. Beyond this limited use, this report may not be shared, distributed, or reproduced without prior written consent from both the company and ProcessUnity, Inc. The content of this report is provided 'as is' of the report date. ProcessUnity makes no representations or warranties, regarding the report's completeness, accuracy, or future applicability. Any findings insights presented are intended for informational purposes to support risk assessment and decision-making and should not be relied upon as legal, accounting, or other professional advice.