ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Cybersecurity Program Review

A structured annual review of Odyssey Logistics' cybersecurity program to verify governance, measure maturity, and demonstrate control effectiveness to leadership and stakeholders.

POLICY POL011 | GLOBAL CYBER PROGRAM | UPDATED 8/28/2025

PROGRAM OVERVIEW

Odyssey Logistics conducts a structured annual review of its cybersecurity program. The review assesses governance alignment, audits control effectiveness, measures program maturity against established frameworks, and reports findings and recommended actions to executive leadership and the board.

01
Assess Governance
The review verifies policies, roles, and decision-making structures against governance and strategic goals.

02
Audit Controls
Technical, administrative, and physical controls are tested and validated for effectiveness.

03
Measure Maturity
Program maturity is scored against an established model, and risk posture is evaluated with audit evidence.

04
Report & Improve
Findings, maturity scores, and gaps are reported to leadership and drive the following year's improvements.

FRAMEWORK ALIGNMENT

NIST CSF
Govern function — program alignment and maturity tiers.

ISO/IEC 27001
Management review and internal audit of the security program.

Maturity Model
Defined scoring to assess program progression year over year.

WHAT THIS POLICY COVERS

The policy is structured across the sections below. Each is mapped to the corresponding area of recognized security practice — demonstrating coverage without disclosing internal control specifics.

§1.1 1.2 **Purpose & Scope**
Annual review across global cybersecurity functions, processes, and controls.

§2.1 **Annual Review Objectives**
Governance alignment, maturity measurement, and gap identification.
NIST CSF · Govern

§2.2 **Review Components**
Governance, control audit, maturity, risk, compliance, and evidence.

§2.3 **Roles & Responsibilities**
CISO oversight, team participation, and independent validation.

§3 **Reporting & Follow-Up**
Board reporting with tracked, prioritized action items. ISO/IEC 27001

§3.1 **Continuous Improvement**
Outcomes inform planning, resourcing, and risk decisions.

Supporting document control: maintained revision history and a referenced documents register.