# Loft Company

Report: NIS2
Loft Company NIS2 + Core Questions + Audit + Essential + Audit + Essential + Policy + Risk Management + Security Measures + Incident Management + Third Party Providers + Testing Audit
v1.0.2026-11-14

Created: 2026-11-14 00:08
Closed: 2026-11-14 00:23
Answered: 98%

Compliance Score:

98%

(453/462)

Almost all requirements met; very low risk.
A very little uncertainty due to small fraction of measuring points not addressed.

---

## Top Risks:

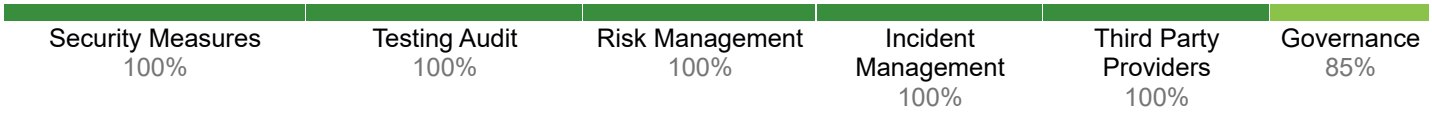
**Governance** – 25% Compliant
1. Are responsibilities for cybersecurity clearly defined and assigned? Unanswered
Criticality: High
2. Does the organization have a documented cybersecurity policy in place? Partially
Criticality: High

---

## Compliance By Section:

| | | | | | |
|---|---|---|---|---|---|
| Governance | 85% | Risk Management | 100% | Security Measures | 100% |
| Incident Management | 100% | Third Party Providers | 100% | Testing Audit | 100% |

## Sections, Weighted




## Compliance by Criticality

| Criticality | Measurement Points | Yes | Partially | No | Missing | Compliance % |
|---|---|---|---|---|---|---|
| High | 61 | 59 | 1 | 0 | 1 | 97 % |
| Medium | 24 | 24 | 0 | 0 | 0 | 100 % |
| **Total** | **85** | **83** | **1** | **0** | **1** | **98 %** |

## Criticalities, Weighted

## Governance

*Covers the organization's governance and management structures for cybersecurity and operational resilience, including roles, responsibilities, and policies.*

| | |
|---|---|
| Does the organization have a documented cybersecurity policy in place? | **Partially** |

Criticality: High

| | |
|---|---|
| Are responsibilities for cybersecurity clearly defined and assigned? | **Unanswered** |

Criticality: High

| | |
|---|---|
| Is there a process for management review of cybersecurity performance and compliance? | **Yes** |

Criticality: High

***<< The rest of this section is left out in this sample/preview >>***

# Recommendations:

## Governance

*Covers the organization’s governance and management structures for cybersecurity and operational resilience, including roles, responsibilities, and policies.*

### 1. Maintain a documented cybersecurity policy.

Criticality: High

### 2. Clearly define and assign cybersecurity responsibilities.

Criticality: High

---

---

Compliance Score: 98% (453/462)
Almost all requirements met; very low risk.