

2023 Cybersecurity Annual Report to Board of Directors

April 2024

Dear Members of the Board,

I am pleased to present the Annual Cybersecurity Report for [COMPANY]

Cybersecurity is a critical function at the intersection of people, processes, and technology. In [Industry], customer [Types of data] can be interrupted, and even compromised, when a cyberattack occurs. That means cybersecurity in [industry] involves more than securing systems and data. It includes protecting customer privacy and data security. We are always mindful that there is a customer at the end of everything we do.

[Industry] cybersecurity has become more critical than ever as the number of digital transactions and connected devices grows, and [Industry] expands into more online and mobile services. Ensuring customer privacy and security in these digital settings is critical. At the same time, cybercriminals continue to attack banking entities with attempts to extort money, steal intellectual property, and cause disruption.

At [COMPANY], we are on a journey toward advancing cybersecurity maturity in our products and enterprise information technology (IT). We recognize that cybersecurity threats continue to evolve, and the strategies, processes, and tools we use must continue to advance. By protecting our customers' information, safeguarding our capabilities and defending the company’s IT infrastructure, we are helping to maintain a thriving and resilient system.

Overall, the past year has been successful in terms of cybersecurity. We have implemented several new measures to strengthen our defenses and respond to emerging threats. The following report outlines our year in review for 2023 and a look into 2024 and beyond.

Overall, I am confident in the strength of our cybersecurity posture. However, we will continue to monitor for and address new threats as they arise, and we will also continue to invest in the training and resources needed to ensure that our defenses remain strong.

Thank you for your support and attention to this important issue.

Sincerely,

CISO, [Company]

## Table of Contents

[*The state of Cybersecurity 4*](#_heading=h.30j0zll)

[*Cybersecurity at [Company] 5*](#_heading=h.1fob9te)

[*Audits and Assessments for 2023 6*](#_heading=h.2et92p0)

[*Best Practice Alignment 7*](#_heading=h.3dy6vkm)

[*Program Maturity and Compliance 8*](#_heading=h.1t3h5sf)

[*Risk Appetite Statement 9*](#_heading=h.2s8eyo1)

[*Inherent Risk Profile 10*](#_heading=h.3rdcrjn)

[*Analysis 11*](#_heading=h.lnxbz9)

# The state of Cybersecurity

Include relevant cyber events that happened in client’s industry and how it is being monitored at the client

# Cybersecurity at [Company]

Give a narrative of how security is going at the client. What are the Strengths, Weaknesses, Opportunities for Improvement.

# Audits and Assessments for 2023

Detail any assessments that were performed during the year and highlights from the assessments. This includes Audits, Penetration Tests, Table Top Exercises, etc.

# Best Practice Alignment

Create a narrative of best practice alignment or compliance coverage. Such as:

The NIST CSF provides a comprehensive and flexible framework that enables organizations to assess and improve their cybersecurity posture in alignment with their unique risk landscape, regulatory requirements, and business objectives. By leveraging the NIST CSF, we gain a structured approach to managing cybersecurity risks, allowing us to identify, protect, detect, respond to, and recover from potential threats and incidents.

The CSF version 2.0 contains 106 controls. These controls are divided into six domains:

* Govern - The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
* Identify - The organization's current cybersecurity risks are understood.
* Protect - Safeguards to manage the organization's cybersecurity risks are used.
* Detect - Possible cybersecurity attacks and compromises are found and analyzed.
* Respond - Actions regarding a detected cybersecurity incident are taken.
* Recover - Assets and operations affected by a cybersecurity incident are restored.

| NIST CSF 2.0 Domain Coverage |
| --- |
|  | Govern (GV) | Identify (ID) | Detect (DE) | Protect (PR) | Respond (RS) | Recover (RC) |
| Implemented | 97% | 66% | 100% | 71% | 100% | 57% |
| Partial | 0% | 33% | 0% | 29% | 0% | 43% |
| N/A | 3% | 0% | 0% | 0% | 0% | 0% |

# Program Maturity and Compliance

Detail overall security program maturity and compliance.

# Risk Appetite Statement

State security’s understanding and alignment to the client’s risk appetite.

# Inherent Risk Profile

Discuss the inherent risk that the client faces due to industry, complexity, location.

# Analysis

Discuss security program goals and risk targeting to summarize the different sections of the report.