CYBERSECURITY

Audit Checklist

Goal

This assessment aims to understand NARO's current network comprehensively and will develop a tailored plan to strengthen the company's defense.

Our checklist will include

Questions based on key elements of the Updated NIST Framework and additional information about the company's current policies

By: Khoa Nguyen, Isaac Caldera, Ronald Dewees

Introduction

This document serves as a cybersecurity audit checklist for the NARO organization, which will record the current status, standards, and procedures of the NARO in compliance with the NIST overall framework.

Based on the criteria and information collected from this checklist, we will develop an exhaustive scan that details the current NARO system's strengths and vulnerabilities. We will also develop procedures and training plans for your employees to mitigate these vulnerabilities.

Identify

These questions will help determine the company’s working environment and understand and manage critical information and potential cyber risks.

1	Do you conduct background check on your potiential employee before hiring them? (yes/no)	
2	Do you revoke former employees' access to company devices/workstations once they no longer work here? (yes/no)	
3	Do you classify your information/data based on their value and sensitivity? (yes/no)	
4	Do you store these critical data on the same server? (yes/no)	
5	Are your management employees understand how critical these data are to the organization? (yes/no)	

6	Do you usually conduct assessments on your devices, including servers, laptops, and workstations in the vehicle bay? (yes/no)	
7	Are there any potential risks related to the material's hazard in the engineering building? (yes/no)	
8	How often do you conduct assessments on the company's critical data? (daily, weekly, monthly, other)	
9	Does the NARO server room in the administration building allow access to all NARO employees or only certain personnel? (yes/no)	
10	Can GAS employee also gain access to NARO server? (yes/no)	
11	Are personal devices (ex: cell phones, tablet,...) allowed on the Engineering office? (yes/no)	
12	If yes, do you have “No Photos” policy on the worksite?	
13	Do you allow employees to carry work laptops out of the business premises? (take home,...)	

Protect

These questions will assess NARO's current protection plan, evaluate it, and establish appropriate measures to reinforce the company's cyber defense.

1	Are there web and email filters in place? (yes/no)	

2	Are your business systems up to date with latest software updates if yes how often? ((yes/no)	
3	Does the NARO manually dispose of its old hardware itself or hire an outside contractor? (self/ contractor)	
4	Have you reset original router administrative passwords? (yes/no)	
5	Do you have a process to securely dispose confidential sensitive documents? (yes/no)	
6	Are the administrative building doors locked outside business hours (9 AM - 5 PM)? (yes/no)	
7	Are security cameras installed at entry and exit points on the administrative and engineer building? (yes/no)	
8	Are security cameras installed in the server room?(yes/no)	
9	Is an access card and administrative permission required to enter the server room? (yes/no)	
10	Do company devices have trackers or auto-lock features in case they are lost or stolen? (yes/no)	
11	Are NARO currently using any anti-virus software? (yes/no) If yes, please specify the software name.	
12	Does management regularly review log access when company employees log in to their work stations? (yes/no)	
13	Are engineering employees allowed to access the administrative building and workstation on that side? (yes/no)	

14	Are company computers and other hardware properly secure when not in use? (yes/no)	
15	How often do you change the PIN access keypad to the secure area? (daily, weekly, monthly, other)	

Detect

These questions will assess NARO's capability to identify and analyze current cyber events, including, but not limited to, external intrusions, internal vulnerabilities, and security breaches.

1	Does management review employees installed software on their personal work device? (yes/no)	
2	Can employees install the software without the need of getting approval from management? (yes/no)	
3	Is there an automatic alert system in case of unauthorized access on company devices and secure areas? (yes/no)	
4	Do you monitor network traffic for unusual data transfer/usage activity on the company network? (yes/no)	
5	Do you track employee web navigation on work devices/networks? (yes/no)	
6	Does NARO restrict access to certain websites on the company network and devices? (yes/no)	
7	Does NARO, Inc. have an automatic system to detect intrusion into the company's security system? (yes/no)	

Respond

These questions help determine business action when disaster strikes with key roles laid out for a organized solution.

1	Is there a chain of command when security breaches occur? (yes/no)	
2	If yes, is there set roles for contacting appropriate enforcement and related contacts? (yes/no)	
3	Are employees trained to report suspicious activity of their co-workers anonymously? (yes/no)	
4	Do you have a primary communication line for both NARO employees and management(Ex: Slack, Discord,...)? (yes/no) If yes, please specify	
5	In case the primary communication line is compromised, does NARO have an alternative secure communication method? (yes/no)	
6	Does your business identify what is defined as a security incident?	
7	Does NARO have procedures to respond to unauthorized access attempts? (yes/no)	
8	Does NARO have a plan to isolate the threats and lock down the server in case of a cyber attack? (yes/no)	
9	If yes, how often does NARO conduct training drills on these mentioned scenarios? (yes/no or N/A if non-applicable)	
10	Has NARO ever been breaches before? (yes/no)	
11	If yes, does NARO still keep records of these past breaches? (yes/no)	

Recover

These questions help determine business action when disaster strikes with key roles laid out for a organized solution.

1	Does NARO backup critical data? (yes/no)	
2	If yes to 1, are these backup data stored on the same server room as regular data?	
3	If yes to 1, are all the backup data stored on the same single location?	
4	If no to 3, how many different locations/servers do you save your data in?	
5	If yes to 1, how many employees know the details and location(s) of where these backup data are stored?	
6	Is there a plan to recover critical data in case the NARO server is compromised? (yes/no)	
7	Is there a priority in recovering these information? (yes/no)	
8	How often does NARO conduct backup on the critical data? (daily, weekly, monthly or N/A if non-applicable)	
9	Does NARO conduct tests on backup data? (yes/no or N/A)	
10	How often does it conduct tests on backup data? (daily, weekly, monthly, other)	

Overall

The information gathered from this checklist will help our company thoroughly understand current policy and assess NARO's potential security risk. This will later allow us to conduct an exhaustive scan further and address any discovered weaknesses of the current policy.