|  |
| --- |
| NARO, Inc  Assessment Report  Prepared by: Jane Doe, John Smith, Juan Perez, Joe Borg |
| **Death Star Consulting** |



# Executive Summary

This is the executive summary. This should be 2-4 paragraphs that provides the high-level, non-technical overview of the report. It should include the background, very short summary of the activities, any critical findings, any conclusions or future work.

Also, the last paragraph should be a short “Thank you” to the individuals at the organization, or contractors, or whoever, that assisted with the assessment. Acknowledge their assistance – it always helps in the future.

Contents

[1 Executive Summary 2](#_Toc97738899)

[1 Introduction 4](#_Toc97738900)

[1.1 Background 4](#_Toc97738901)

[1.2 Scope 4](#_Toc97738902)

[1.3 Report Organization 4](#_Toc97738903)

[2 System Overview 5](#_Toc97738904)

[2.1 Facility or System 1 5](#_Toc97738905)

[2.2 Facility or System 2 5](#_Toc97738906)

[2.3 Facility or System 3 5](#_Toc97738907)

[3 Assessment Methodology 6](#_Toc97738908)

[4 Assessment Activities 7](#_Toc97738909)

[4.1 NARO Documentation Review 7](#_Toc97738910)

[4.2 In-person Interviews 7](#_Toc97738911)

[5 Assessment Results and Recommendations 8](#_Toc97738912)

[5.1 Weaknesses 8](#_Toc97738913)

[5.2 Strengths 9](#_Toc97738914)

[5.3 Observations 9](#_Toc97738915)

[6 Conclusions and Follow-on Activities 10](#_Toc97738916)

# Introduction

Quick introduction to this section. This section includes…

## Background

Why is this assessment happening? For example:

AOTIR, Inc. (Another Organization That Isn’t Real) that provides services similar to NARO, Inc. suffered a ransomware attack, taking their business offline for 2 months while they recovered. To reduce their risk of this happening to their organization NARO, Inc. (NARO) decided they needed to conduct a cybersecurity assessment. Etc.

## Scope

What was in-scope for this assessment, what was out-of-scope for this assessment, and things looked at. This includes any limitations to the assessment. In a hands-on assessment, production systems might be out-of-bounds, so this would be mentioned here.

## Report Organization

The rest of this report is organized as follows: Section 2 provides an overview of the NARO facilities, systems, and processes used. Sections 3 and 4 describe the methodology used by the team and the activities they conducted. The assessment results are found in Section 5, with conclusions and recommended follow-on activities in Section 6. Appendices include additional information related to the assessment.

# System Overview

The introduction to this section should have 1-2 paragraphs about the overall system. It’s overall purpose, facilities, etc.

## Facility or System 1

This is a description of the first system or facility. There are a variety of ways to organize this breakdown, and it will depend on what seems the best for each assessment – and the recipients of the report. For example, if you look at multiple types of systems at multiple facilities, it may depend on how the organization has their areas of responsibility. For example, at UTSA, if you were looking at the various IT systems deployed around campus, you might break it down by functionality – email, wireless access, etc. If you were looking at fire detection and suppression systems – smoke detectors, sprinklers, emergency alerts, fire extinguishers – it might make sense to break it down by buildings since they were constructed at different times and probably have different systems installed. Plus, some buildings may have special requirements (like storing chemicals) which a standard office building wouldn’t be worried about.

**Key items**:

This should provide enough information that all of your findings can trace back to this section. That way, if information is incorrect, you can trace back to where it went wrong. Plus, in 5 years, the source information may be shredded and gone – and only this report is left to reference.

Also, this section should be factual and descriptive. This isn’t the section to say something is good/bad/whatever. Also, if you don’t KNOW something, but THINK it is a certain way – make sure you state that.

## Facility or System 2

Etc.

## Facility or System 3

Etc.

# Assessment Methodology

The intro to this section should be something like: “The team used the Death Star Consulting (DSC) SBNP methodology. This methodology was developed specifically for small businesses and non-profit organization to address security concerns and other issues that are often found in smaller organizations, but are addressed in very different ways in large corporations.

This majority of this section can probably be taken from Assignment #1. Your team can decide how you want to use, combine, or incorporate the various work from the group members. Or, you can come up with something completely new. Just make sure it addresses things like you were asked to do in Assignment 1.

# Assessment Activities

The introduction should simply state that this section covers the high-level activities performed by the assessment team. It should also state that the observations and findings made from these activities are discussed in Section 5.

## NARO Documentation Review

Each of these assessment activities should be fairly short – unless there is something very detailed or nuanced. For example, if you were removing chips from a motherboard, dumping their firmware, and reloading the firmware with malicious versions – that would probably be a much longer description. However, if you were just reviewing documentation provided by an organization, you could keep it to 1-2 paragraphs. If there are a lot of documents, you could list them (including version numbers and dates) in an Appendix.

## In-person Interviews

On whatever date, the team met with WHOEVER from NARO, Inc. to discuss…

# Assessment Results and Recommendations

The intro to this section should discuss that the results obtained from the assessment activities in Section 4 are in this section. It should also mention that this section will include strengths, weaknesses, and observations.

Strengths are things they are doing well. This is to give them some good news to go with the bad news. Plus it makes sure they don’t stop doing those things as they mitigate the weaknesses.

Weaknesses are things that could be a vulnerability, or otherwise help out an attacker. For example, they could be running an older version of Windows, or outdated antivirus. Or, it could be something like the cleaning company has keys to the buildings, but has no idea who should be allowed in the building – so someone could gain unauthorized access. Also, weaknesses should have a severity rating. There are many different rating systems out there – from the simple, to the incredibly complex. (I have used one that required multiple spreadsheets to calculate the overall score based on CVSS scores and other inputs.) I recommend you use HIGH, MEDIUM (or MODERATE), and LOW to keep it simple.

Observations are things that are not strengths or weaknesses, or doesn’t have enough information to really make a determination. So, imagine it was a hands-on assessment, but you couldn’t touch the production systems since they are supporting critical business operations. If you notice that one of those systems is unlocked, and no one is around, it is probably bad – but it is out of scope, so you don’t call it a weakness. Because, for all you know, someone made the lock screen image look like the desktop as a joke.

Also, if you do this professionally – do NOT go outside of your rules of engagement and the scope of the assessment. It doesn’t matter how cool something looks, or seems like you could compromise a system in 5 minutes. (Also, never do work without a rules of engagement that has been signed by the cognizant authority.)

## Weaknesses

**(High) Backups of critical systems and data has not been performed in over 2 years.**

Justification: A lack of backups means that systems can not be restored in the event of a ransomware attack or system failure. Manually entering the information from paper files would take approximately 3 months.

Mitigations: Create a backup procedure that is followed on a regular basis. This should include off-site storage of backups, encrypting the backups to ensure the data is secure when taken off-site, and regularly testing that the systems and databases can be restored from the backups.

NOTE: Each finding/weakness should have more detail, providing enough information to support your severity rating. In addition, the mitigation(s) should specifically address this issue. Keep each one “self-contained” where someone trying to fix a specific issue has all the information in the finding.

## Strengths

**Physical Security**:

* Only the facility manager, assistant manager, and CEO have keys to access the building and the code to disarm the alarm system.

**Backups**:

* Daily backups are stored on AWS, and a weekly backup is made using an Ironkey flash drive which is taken off-site to the company safe deposit box at a local bank branch. In addition, both procedures are conducted by two people who verify it was completed correctly, and report the successful backup by sending an email to the CEO.

## Observations

**Employees use their personal mobile devices to access work systems**

Description: Employees are able to use their personal devices to access work systems such as email, calendar, time reporting, and most work functions. However, it was unclear if all of those functions required the third-party application that was selected to ensure the security of that data on their device, and when it was transmitted over the internet.

Recommendation: Review the use of work services on employees personal devices to ensure that all work-related activities are secured in an appropriate manner, and in accordance with NARO policies.

# Conclusions and Follow-on Activities

The first paragraph should include a high-level summary of the assessment. Something like:

The assessment team found NARO applies industry best practices across all of their facilities, systems, and procedures. However, the team did identify several vulnerabilities that could be used by an attacker to compromise NARO systems and information. Of the vulnerabilities identified in Section 5, the team recommends the vulnerabilities related to backups be prioritized given the concerns related to ransomware attacks common to this business area.

For follow-on activities, the team recommends…