CS-3113-01T
Course Project
Cybersecurity Assessment for NARO Inc.

In-Brief Presentation

DEATH STAR CONSULTING

DAMIEN BELTRAN, HANNAH STANEK, ISAIAH ALVAREZ, WES GAUSE

What is An Assessment?

A cybersecurity assessment is a structured evaluation of an organization’s ability to protect its systems, data, and operations from cyber threats.

At NARO, this assessment will help identify security gaps across areas such as network access, data handling, physical security, and remote connectivity without disrupting day to day operations.

This assessment follows NIST recommended best practices and is tailored to NARO’s specific environment, including its R&D activities and limited IT resources. As your consulting company, Death Star Consulting is here to support informed, risk based decisions that strengthen your cybersecurity posture.

ROADMAP

1 — 2 — 3 — 4 — 5 — 6

1 Project Plan

Death Star Consulting assessing the plan of execution for the team to start your cybersecurity assessment

2 In-Brief

Gives us an opportunity to sit down with you and speak about what it is that we will do for you. Provides an opportunity to address high level expectations for the assessment

3 Audit Checklist

Our Audit Checklist will guide us through key areas such as network security, remote access, physical controls, and system configurations.

4 Assessment Activities

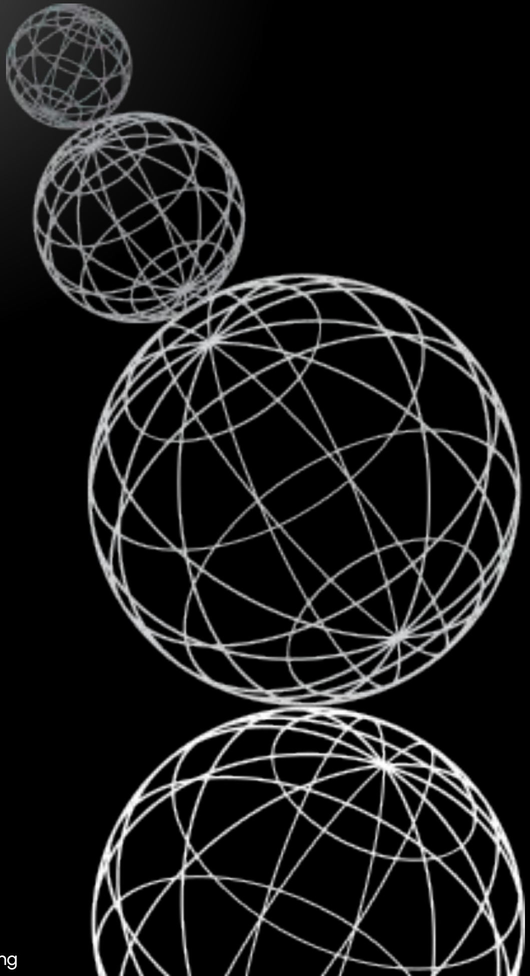
Provide a thorough checklist of activities to be accomplished. Review materials provided, initiate interviews with team members as well. Finally address follow up questions reviewing key insights.

5 Assessment Report

Evaluations will be made on policies and procedures. Assessment of communication through key services Naro focuses on. Evaluate cyber security training and systems.

6 Out-Brief

Allows the opportunity to discuss key factors from the assessment. Review findings, potential mitigations, and most importantly conclusive details and recommendations.



In-Brief

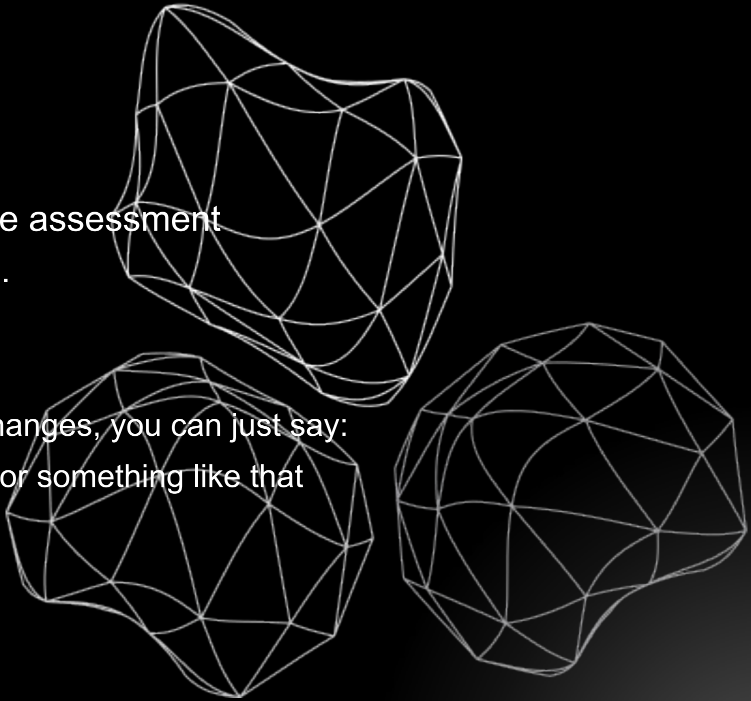
For a brief overview of our engagement with NARO Inc., This in-brief marks the beginning of our collaborative cybersecurity assessment effort.

As assessors from Death Star Consulting (DSC) we aim to, Walk you through the cybersecurity services we provide. Customize a paper-based assessment to fit your organization's structure and needs. Understand you priorities and concerns, especially around your unique operational environment.

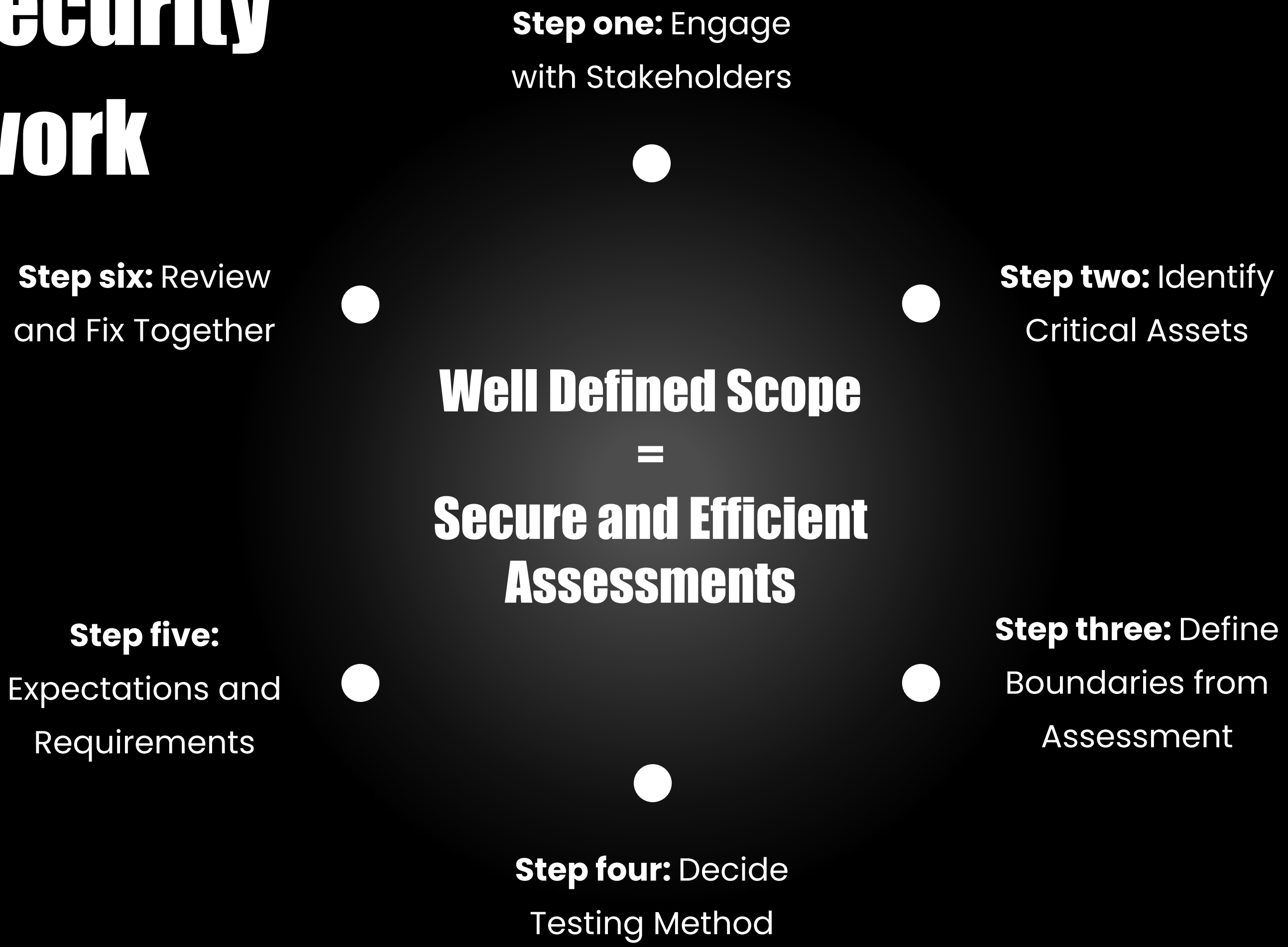
No active testing will occur as this will be planning focused, non-invasive assessment. We're here to listen, analyze, and advise.

Determine Scope

- This is a short list and description of what you did for the assessment
- If you reviewed documents, then you would describe that here.
- If it is a short list of documents, you might also include that list
- This should also include any interviews or discussions
- You don’t have to get too detailed – if you had 5-10 email exchanges, you can just say:
- “Emails were also exchanged to answer follow-on questions.” or something like that



CyberSecurity Framework



Step one: Engage with Stakeholders

Step two: Identify Critical Assets

Step three: Define Boundaries from Assessment

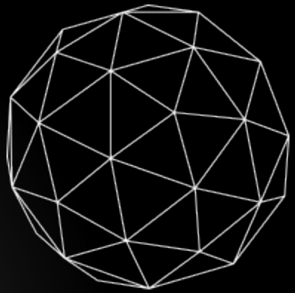
Step four: Decide Testing Method

Step five: Expectations and Requirements

Step six: Review and Fix Together

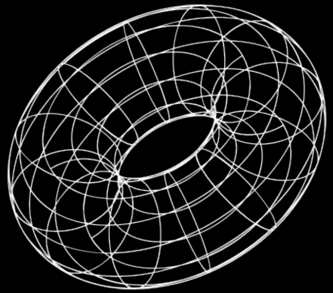
Well Defined Scope = Secure and Efficient Assessments

POLICY ASSESSMENT



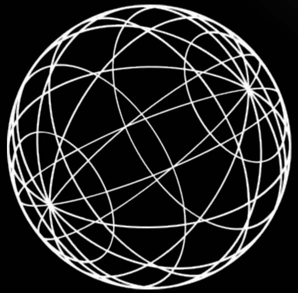
Remote Access Policy

Documents which users are being connected to the organization's internal networks. This policy ensures secure and controlled access while protecting sensitive information and systems from potential threats.



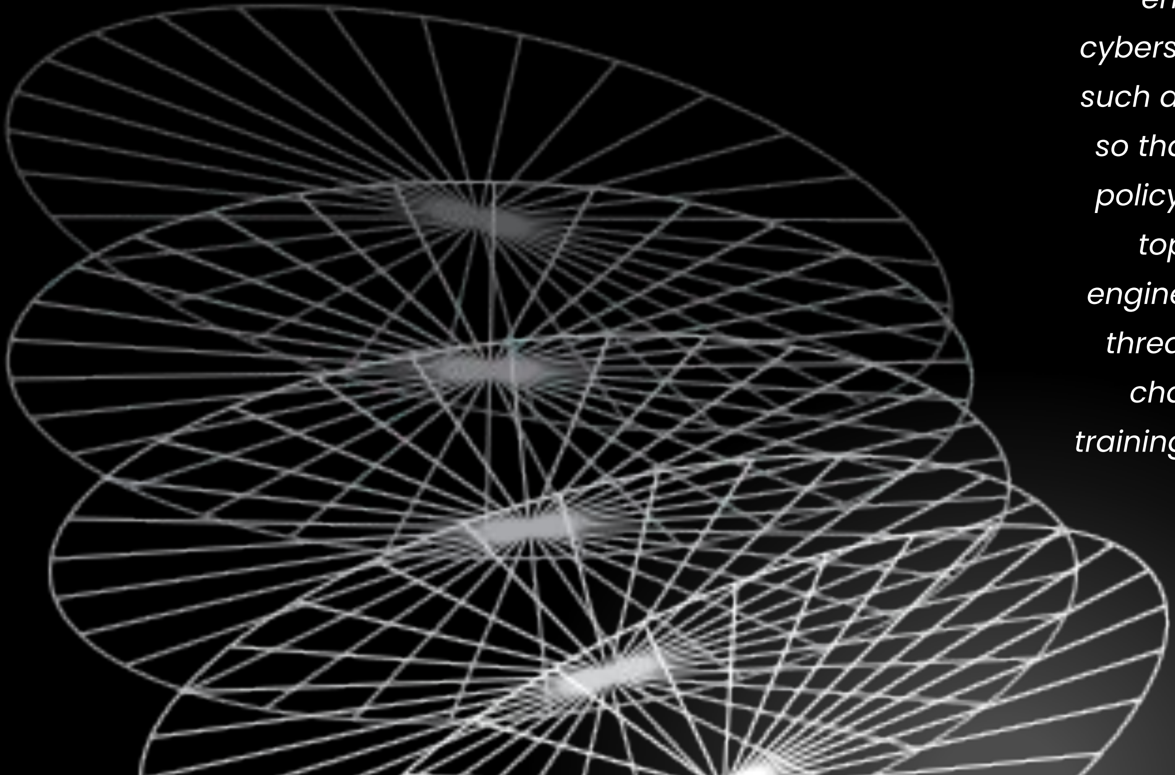
Email and Communications Policy

Rules and regulations set by the organization relating to sending emails or the use of any other communication channels. This policy ensures professional conduct while also protecting sensitive information. It also prevents misunderstandings from occurring, as well as self reputational damage.



Incident Response Policy

Preparation for the detection, containment, eradication, and recovery phases that come from security incidents. Brings awareness of threats to employees and trains them to stay calm while effectively counteracting attacks.



Training Assessment

The industry standard for many organizations include training that reinforces the policies an employee is expected to know. During cybersecurity assessments, training programs such as these should be thoroughly inspected so that the training still falls under company policy. These training programs can contain topics such as email safety and social engineering. The cyberspace is ever evolving, threats are always lingering around for the chance to strike, hence why continuous training is essential to ensure an organization’s workforce is kept in the know.

NIST Cybersecurity Framework: Core Principles

“If you think tech will solve your security problems, you don’t understand either.”
— *Bruce Schneier, Cryptographer and Security Technologist*

Identify

Know what matters

To protect an organization, it is vital to understand its assets, the risks they face, and the environment in which they operate.

Protect

Secure by design

Through the implementation of safeguards that protect your company's assets we can ensure that security is implemented consistently throughout your organization.

Detect

Always aware

Quickly identifying security events is critical to minimizing the impact of bad actors and sustaining business operations.

Respond

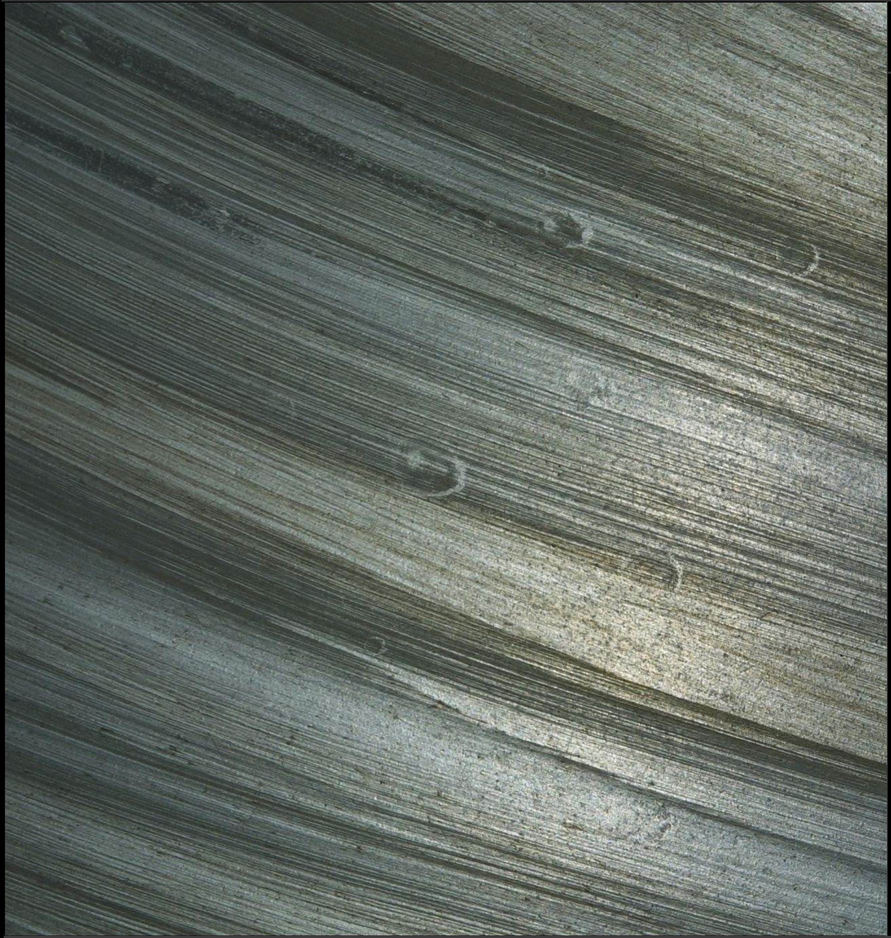
React with purpose

Swift actions taken during emergencies are only possible through proper planning and regular practice.

Recover

Rise Stronger

Quickly restore operations, learn from past incidents, and strengthen your defenses to better withstand future security events.



Tailored Assessment

Our Protocols

- Death Star Consulting's assessment begins with an evaluation of all policies and procedures related to identity and access management.
- We will then assess the security of network all devices to include any remote access technologies implemented within your organization.
- We will also evaluate the effectiveness of your employee cybersecurity training programs.
- Our review will cover all policies and technologies related to physical security and data retention.
- Upon completion, we will deliver a detailed report that lists our findings, along with recommended mitigations and remediation strategies that we suggest.

Out-Brief

FIN/ACK

At Death Star Consulting, we are committed to our clients and protecting their data. Once the assessment has been concluded, we will provide a comprehensive final report detailing all findings, along with any remedial actions that we recommend. We will collaborate with the appropriate personnel to ensure that any temporary system changes are reversed, including the removal of temporary user accounts and scripts. In line with our commitment to NARO's security and in accordance with our company's data retention policies, all client data will be encrypted and securely stored in our system for two years.