NIST Initial Assessment Report

[Anonymized]

Please be informed that this is an incomplete version of the NIST Cybersecurity Framework Assessment

Get full report

Table of contents

Table of contents

Executive Summary

[Name of company] has requested that UnderDefense, as an independent and trusted Cyber Security partner, conducts an assessment and analysis of the current state of the information technology security program of the organization and its compliance with NIST Cybersecurity Framework. The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks.

The result of UD assessment is a report which concludes with thoughtful review of the threat environment, with specific recommendations for improving the security posture of the organization.

Our methodology

Our methodology is based on the interviews and practical evaluation with the key stakeholders and reviewing technical documentation. All the findings are mapped on NIST CSF standard (see below). Rating provided in form of Maturity Level matrix and Radar chart.

Key stakeholders interviewed

The first important step of our assessment was the interview with the key stakeholders and employees to collect information and check on practice the current control set and the risks that knowledge keepers observe in the organization.

The following table represents a list of individuals who took part in the interview. The respondents shared the information regarding information security in their organization, presented current controls of information security in their departments and answered questions from NIST CSF checklist regarding processes, finance, systems, infrastructure, business processes, policies, growth plans, endpoint security, operating systems, access controls, valuable assets, risks, etc.

Position in the company	Respondent

NIST CSF Information Security Maturity Model

A maturity model is needed to measure the information security processes capabilities. The main objective of such maturity model is to identify a baseline to start improving the security posture of an organization when implementing NIST CSF.

	LEVEL 1 - PERFORMED	LEVEL 2 - MANAGED	LEVEL 3 - ESTABLISHED	LEVEL 4 - PREDICTABLE	LEVEL 5 - OPTIMIZED
people	General personnel capabilities may be performed by an individual, but are not well defined	Personnel capabilities achieved consistently within subsets of the organization, but inconsistent across the entire organization	Roles and responsibilities are identified, assigned, and trained across the organization	Achievement and performance of personnel practices are predicted, measured, and evaluated	Proactive performance improvement and resourcing based on organizational changes and lessons learned (internal & external)
process	General process capabilities may be performed by an individual, but are not well defined	Adequate procedures documented within a subset of the organization	Organizational policies and procedures are defined and standardized. Policies and procedures support the organizational strategy	Policy compliance is measured and enforced Procedures are monitored for effectiveness	Policies and procedures are updated based on organizational changes and lessons learned (internal & external) are captured.
technology	General technical mechanisms are in place and may be used by an individual	Technical mechanisms are formally identified and defined by a subset of the organization; technical requirements in place	Purpose and intent is defined (right technology, adequately deployed); Proper technology is implemented in each subset of the organization	Effectiveness of technical mechanisms are predicted, measured, and evaluated	Technical mechanisms are proactively improved based on organizational changes and lessons learned (internal & external)

Conclusions

Radar chart below provides a graphical summary of the assessment outcome. The chart describes the current maturity level of each NIST CSF category. Each maturity level corresponds to numeric level on the chart:

- Level 1 - Performed Process,
- Level 2 - Managed Process,
- Level 3 - Established Process,
- Level 4 - Predictable Process,
- Level 5 - Optimizing Process.

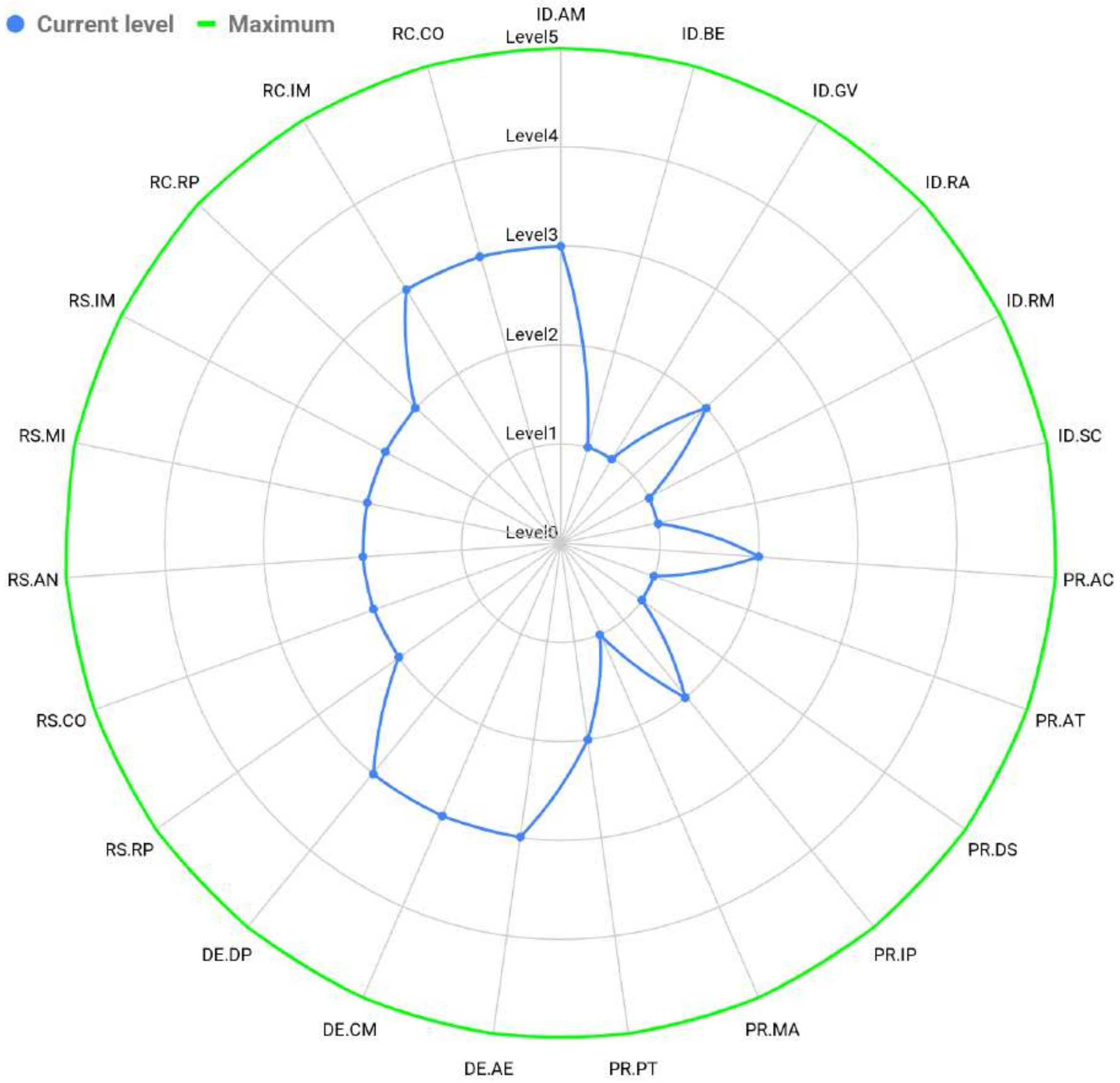

Figure 1. Graphical representation of each maturity level.

RoadMap

[CLIENT] needs to assign roles and responsibilities, to handle all actions related to the analysis of the non-conformity, execution of improvements and controls implementation to achieve the acceptable state for certification.

The table below shows ISO 27001:2013 controls ordered and prioritized by severity of Maturity Levels.

The table represents step by step guide to start executing improvements on minor non-conformity clauses and proceed with major non-conformity. It is highly recommended to follow the order, controls, which marked as Conforms, represent what's already in place and working well, minor non-conformities can be resolved by one-time activities(e.g. waterfall methodology), major non-conformities requires iterative, team-based approach, in order complete all activities, resolve issues effectively and in time.

The table can be treated as a project plan that contents 3 Stages, as presented in the table below, which represent required steps for successful transition and compliance.

Cybersecurity Framework implementation guidance:
Step 1: Prioritize and Scope — Requests that organizations scope and prioritize business/mission objectives and high-level organizational priorities. This information allows organizations to make strategic decisions regarding the scope of systems and assets that support the selected business lines or processes within the organization.
Step 2: Orient — Provides organizations an opportunity to identify threats to, and vulnerabilities of, systems identified in the Prioritize and Scope step.
Step 3: Create a Current Profile — Identifies the requirement to define the current state of the organization's cybersecurity program by establishing a current state profile.
Step 4: Conduct a Risk Assessment — Allows organizations to conduct a risk assessment using their currently accepted methodology. The information used from this step in the process is used in Step 5.
Step 5: Create a Target Profile — Allows organizations to develop a risk-informed target state profile. The target state profile focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes.
Step 6: Determine, Analyze, and Prioritize Gaps — Organizations conduct a gap analysis to determine opportunities for improving the current state. The gaps are identified by overlaying the current state profile with the target state profile.
Step 7: Implement Action Plan — After the gaps are identified and prioritized, the required actions are taken to close the gaps and work toward obtaining the target state.

[Name of company] needs to assign roles and responsibilities, to handle all actions related to the analysis of each assessed category, execution of improvements and controls implementation to achieve the acceptable state. Acceptable state can be identified after Step 4: Conduct a Risk Assessment and Step 5: Create a Target Profile. Creating Target Profile means to define desired Maturity Level for each Category.

Not conducting a Risk Assessment means trying raise each category one level higher or for example raise all categories to LEVEL 4. But keep in mind that it might be economically unprofitable for your company.

The table below shows NIST CSF categories ordered and prioritized by severity of Maturity Levels. The table can be treated as a raw project plan that contents 3 Stages.

№	Assessed Category	Maturity Level
1	**Level 1**	
1.1	Business Environment (ID.BE)	LEVEL 1 - PERFORMED
1.2	Governance (ID.GV)	LEVEL 1 - PERFORMED
1.3	Risk Management Strategy (ID.RM)	LEVEL 1 - PERFORMED
1.4	Supply Chain Risk Management (ID.SC)	LEVEL 1 - PERFORMED
1.5	Awareness and Training (PR.AT)	LEVEL 1 - PERFORMED
1.6	Data Security (PR.DS)	LEVEL 1 - PERFORMED
1.7	Maintenance (PR.MA)	LEVEL 1 - PERFORMED
2	**Level 2**	
2.1	Risk Assessment (ID.RA)	LEVEL 2 - MANAGED
2.2	Identity Management, Authentication and Access Control (PR.AC)	LEVEL 2 - MANAGED
2.3	Information Protection Processes and Procedures (PR.IP)	LEVEL 2 - MANAGED
2.4	Protective Technology (PR.PT)	LEVEL 2 - MANAGED
2.5	Response Planning (RS.RP)	LEVEL 2 - MANAGED
2.6	Communications (RS.CO)	LEVEL 2 - MANAGED
2.7	Analysis (RS.AN)	LEVEL 2 - MANAGED
2.8	Mitigation (RS.MI)	LEVEL 2 - MANAGED
2.9	Improvements (RS.IM)	LEVEL 2 - MANAGED

№	Assessed Category	Maturity Level
2.10	Recovery Planning (RC.RP)	LEVEL 2 - MANAGED
3	**Level 3**	
3.1	Asset Management (ID.AM)	LEVEL 3 - ESTABLISHED
3.2	Anomalies and Events (DE.AE)	LEVEL 3 - ESTABLISHED
3.3	Security Continuous Monitoring (DE.CM)	LEVEL 3 - ESTABLISHED
3.4	Detection Processes (DE.DP)	LEVEL 3 - ESTABLISHED
3.5	Improvements (RC.IM)	LEVEL 3 - ESTABLISHED
3.6	Improvements (RC.IM)Communications (RC.CO)	LEVEL 3 - ESTABLISHED

Appendix A: The Current Framework Profile

The Current Profile indicates the cybersecurity outcomes that are currently being achieved

IDENTIFY (ID) Function

	Asset Management (ID.AM)
Short description	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy
Subcategories	ID.AM-1: Physical devices and systems within the organization are inventoried ID.AM-2: Software platforms and applications within the organization are inventoried ID.AM-3: Organizational communication and data flows are mapped ID.AM-4: External information systems are catalogued ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

UnderDefense
CYBERSECURITY

Please be informed that this is an incomplete version of the UnderDefense NIST Cybersecurity Framework Assessment

If you're interested in accessing the comprehensive version, kindly follow the link provided below.

Get full report

☎ +1 929 999 5101