Case Study

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

NIST Cybersecurity Framework Assessment

Compliance

Solution/Service Title	NIST Cybersecurity Framework Assessment
Client Industry	Software development and customer support services for Apple's Mac OS.
Client Overview	A technology driven company creating products, competing in the global market, from the USA to Asia.
Client Challenge	Establishment of the appropriate levels of governance and management to accomplish the risk objectives, enterprise goals in alignment with organizational drivers such as compliance with external laws and regulations or business service continuity and availability.
Scope	The scope of this assessment is bounded by specified services of company and specified facilities. The in-scope applications, systems, people, and processes are globally implemented, operated by teams and are specifically defined in the scope and bounds.
Key Benefits	UnderDefense created the Current Profile for all of the NIST CSF subcategories. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. UnderDefense helped the client to establish a roadmap that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities.
Results	UnderDefense provided a set of activities, outlined in the Profile guidance and recommendations, in consideration of the unique organizational context. UnderDefense set priorities and identified a baseline to start improving the security posture of the client in alignment with Information Security Maturity Model For NIST CSF.

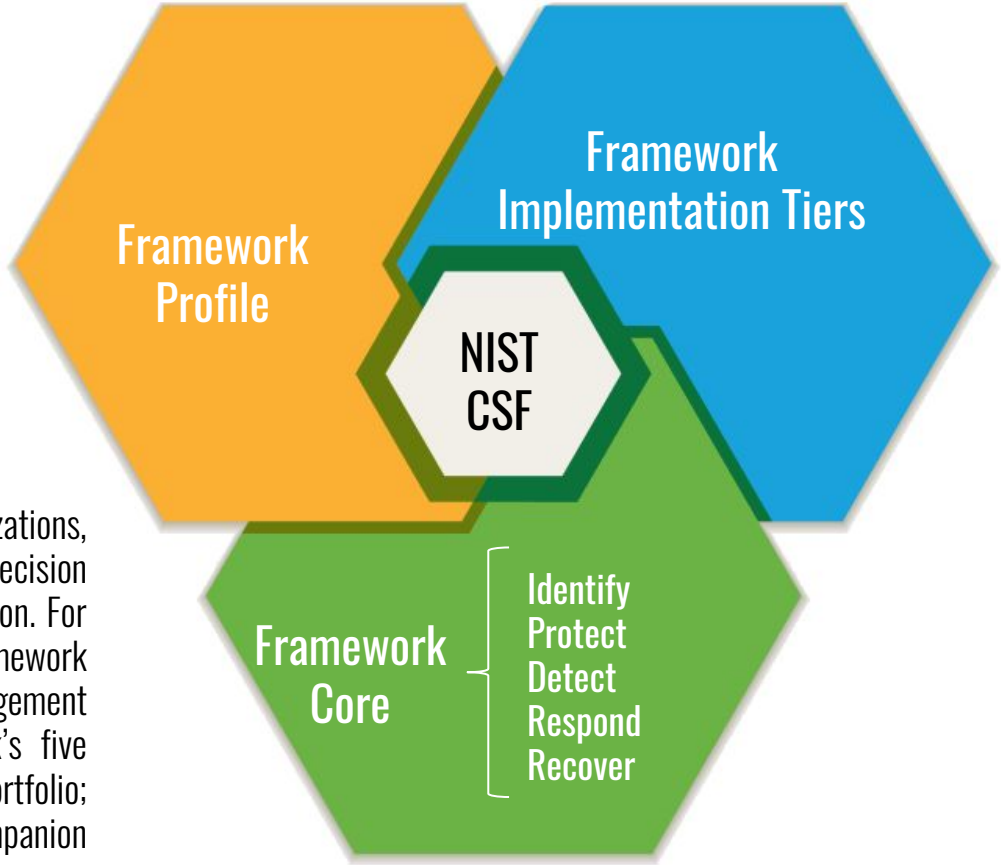
Certifications

Ph.D. in Security

The Framework

The Framework complements, and does not replace, an organization's risk management process and cybersecurity program. The organization can use its current processes and leverage the Framework to identify opportunities to strengthen and communicate its management of cybersecurity risk while aligning with industry practices. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.

To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization. For example, one organization may choose to use the Framework Implementation Tiers to articulate envisioned risk management practices. Another organization may use the Framework's five Functions(Core) to analyze its entire risk management portfolio; that analysis may or may not rely on more detailed companion guidance, such as controls catalogs.



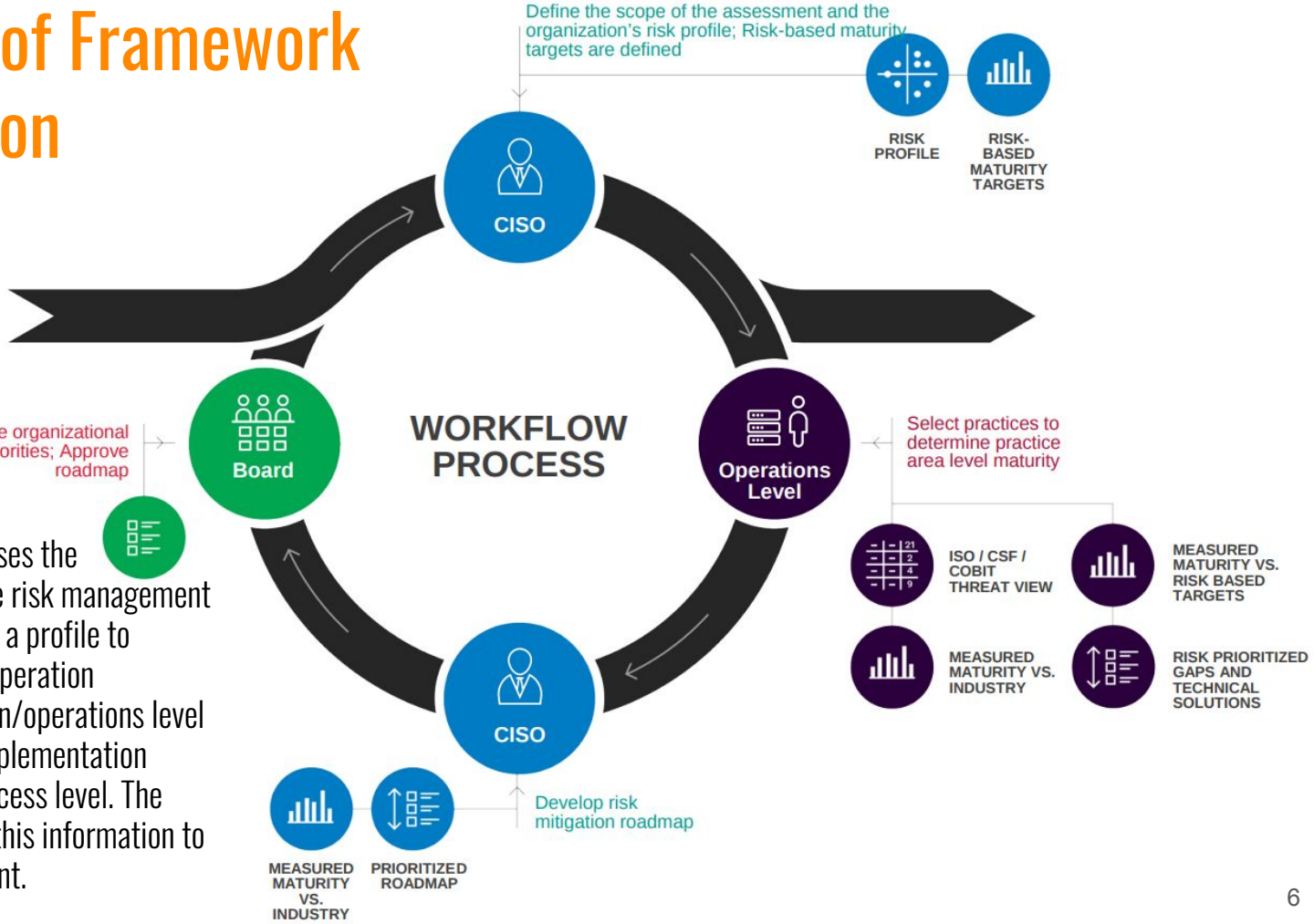
The Framework Core

The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

Coordination of Framework Implementation

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level.

The business/process level uses the information as inputs into the risk management process, and then formulates a profile to coordinate implementation/operation activities. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment.



Team composition

1 ISO 27001 Lead Auditor
2 Cyber Security Auditors

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Assessment Overview

1 Documentation analysis

Informal review of the Cybersecurity Program, for example checking the existence and completeness of key documentation such as the organization's cybersecurity policy, Target Profile or Statement of Applicability (SoA) and Risk Treatment Plan (RTP). This stage serves to familiarize the UD assessors with the organization and vice versa.

2 Interviews phase

A more detailed and formal check, independently testing the Cybersecurity Program against the requirements specified in NIST SP 800-53 Rev. 4, ISO/IEC 27001, CIS CSC. UD assessors will seek evidence to confirm that the technical mechanisms has been implemented and are predicted, measured, and evaluated. The assessors ensure weather policies and procedures are updated based on organizational changes and lessons learned (internal & external) are captured.

3 Security posture analysis

UD team process findings collected during interviews and checks, this is the phase where we write down what we have found during the assessment – names of persons we spoke to, quotes of what respondent said, IDs and content of records we examined, description of facilities we visited, observations about the equipment we checked, etc.

4 Recommendations

Following the evaluation, the team prepare comprehensive roadmap to rapidly eliminate non-conformities, detailed recommendations following the NIST SP 800-53 Rev. 4, ISO/IEC 27002:2013, CIS CSC best practices.

5 Final results

The team deliver Assessment Report, make final presentation that represent key findings and mapped roadmap for future improvements.

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

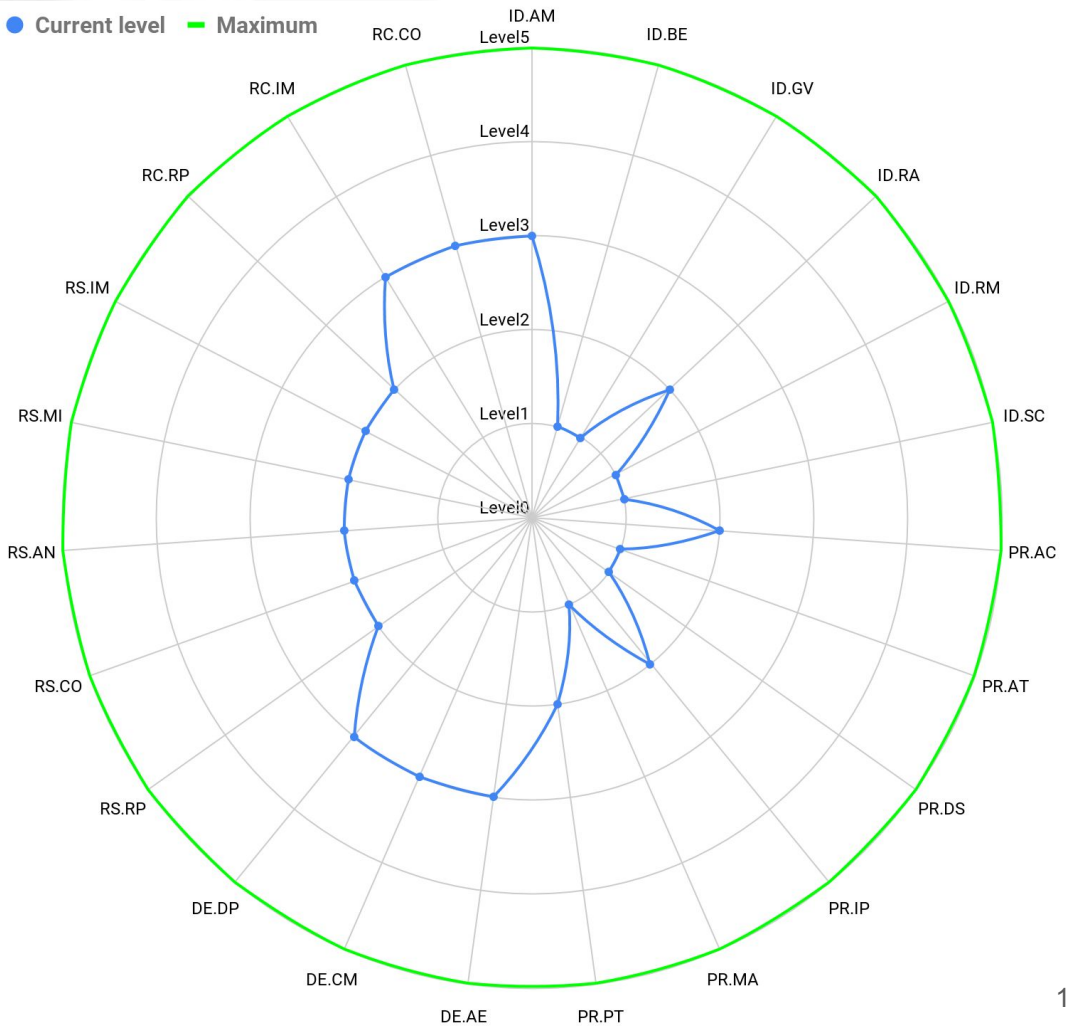
Information Security Maturity Model For NIST CSF

	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)

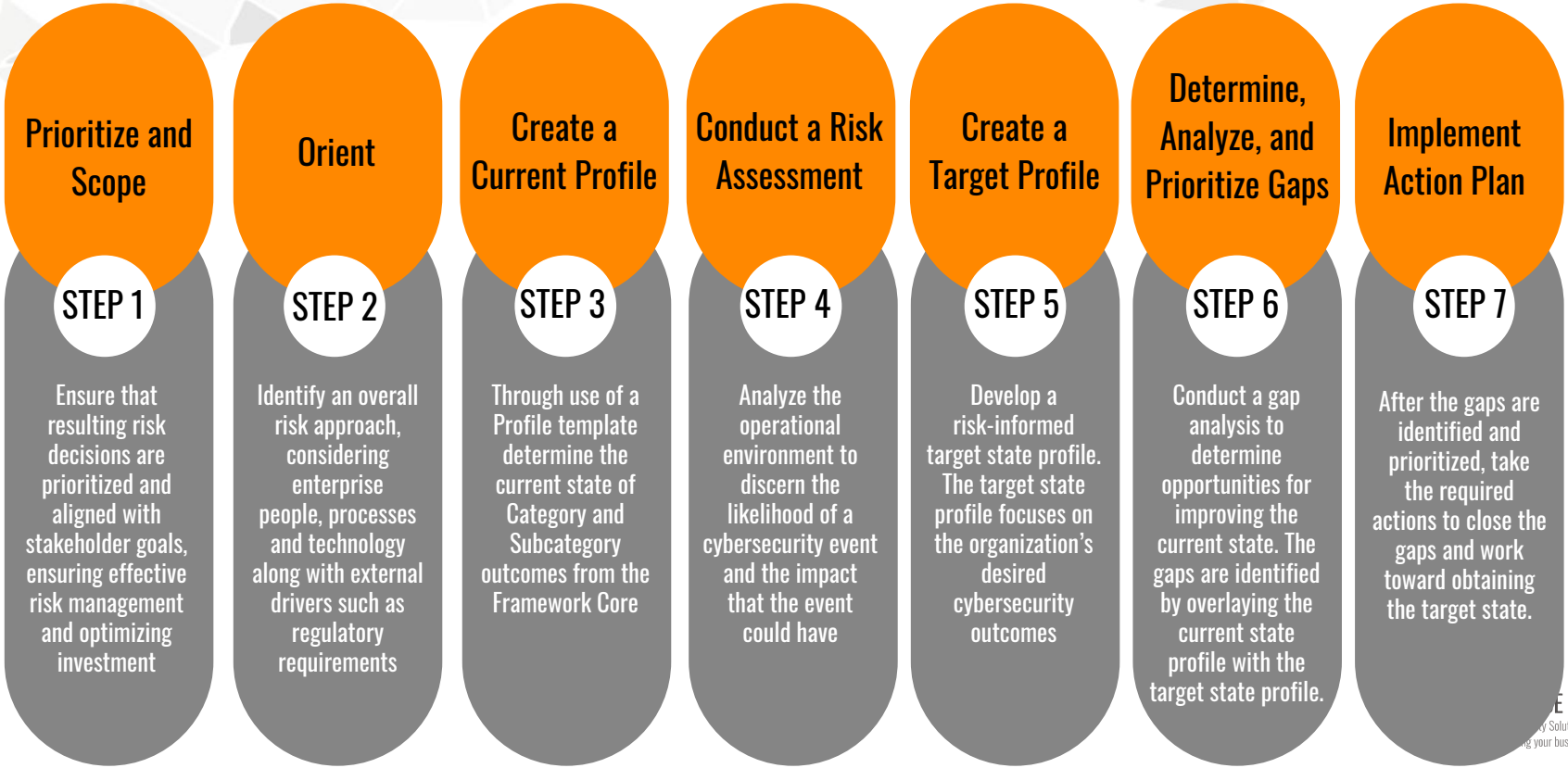
UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Security posture analysis

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.



Framework Implementation



Roadmap

Priorities and Traceability are crucial concepts when achieving Target Profile.

Once you have a score for each item, you can have a fact-based, objective discussion with the team about what is appropriate to do first and what to do second, our prioritized roadmap enabled the client to do so.

Traceability Matrix enabled the client to track transition to higher Maturity Level of each control. The process of framework implementation is transparent and easy to follow.

UNDER DEFENSE
CyberSecurity Solutions
Protecting your business

Get prioritized Roadmap

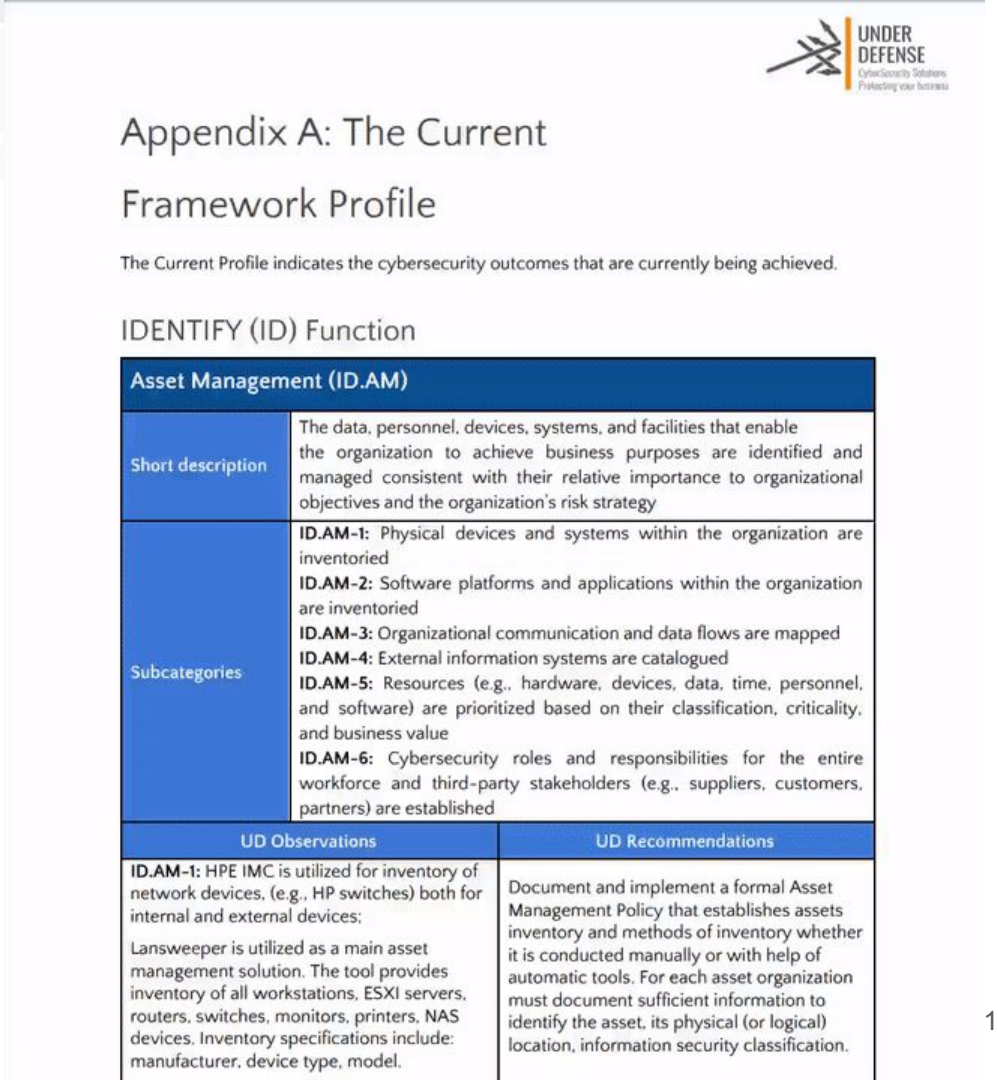
	C	D	E	F	G	H	I	J	K	L
1	Subcategory	Task	Impact on "Unable to release product version"	Impact on "Unable to deliver product version to users/customers"	Impact on "Inability to sell the product"	Impact on "Unable to deliver technical support to our customers"	Impact on "Inability to sell the service"	Impact on "Office unavailability"	Impact on Data Breach	Priority
15	PR.DS-7: The development and testing environment(s) are separate from the production environment	Implement fully functional testing environments, so that test cases can be performed without afraid to cause damage to production environment.	0	3	2	2	2	0	0	199
16	PR.AC-3: Remote access is managed	Set up monitoring remote access to the production system. Allow only authorized use of privileged functions from remote access. Establish agreements and verify security for connections with external systems.	2	2	1	1	1	0	2	194
17	PR.AT-2: Privileged users understand their roles and responsibilities	Establish specific cybersecurity awareness and training procedures for privileged users (e.g. developers) describing acceptable and unacceptable activities at workplace.	2	2	1	1	1	0	2	194
18	PR.DS-1: Data-at-rest is protected	Create and implement procedures which describe how to encrypt all data related to PII within all AWS infrastructure.	0	0	2	1	2	0	3	190
19	PR.AC-2: Physical access to assets is managed and protected	Define, document and implement procedures in Access Control Policy that would describe roles and responsibilities related to physical access. For example: who has to escort fire inspector or air conditioning service during their operations, to what extent, etc;	1	1	1	1	1	3	2	188
20	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	Define and establish formal procedures describing response, recovery planning and testing with suppliers and third-party providers. Include procedures in contracts; Include in contracts a provision that requires your third-party suppliers/partners to notify you immediately if there is a potential or actual security incident, data security breach.	1	1	2	1	1	0	2	183
21	PR.DS-2: Data-in-transit is protected	Create and implement procedures which will describe how data should be transferred. For example which corporate messenger employees should use for communication or how to correctly obfuscate data before transfer or how to choose a protected way for	1	1	1	1	1	0	3	182

Get the Traceability

	E	F	G	H	I	J	K
1	Subcategory	Task	Check if task is done	Maturity Level Achieved	Task Value	Maturity Level Coefficient	Numeric Maturity Level Mark Achieved
31	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Establish Risk Management Process;	☐	LEVEL 1 - PERFORMED	0	2	1
32	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Create Risk Management Framework document that would contain risk factors: threats, vulnerabilities, impacts, likelihoods, risk levels matrix. Consider following: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf Review the documents containing the lists of assets and define a single comprehensive list of assets along with asset owners while considering above mentioned recommendation.	☐		0	2	
33	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	Adjust Risk Assessment Framework so that it includes the criteria for accepting risk and identifying the acceptable level of (e.g. at what level can risk automatically be accepted and under what circumstances). Approval should be obtained from top management for the decision to accept residual risks, and authorization obtained for the actual operation of the ISMS.	☐		0	3	
34	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	Establish policies, procedures, and implement mechanisms to ensure that the information produced during risk assessments is effectively communicated and shared across all risk management tiers.	☐		0	2	

Final results

UnderDefense provide reports with detailed information on identified gaps, their severity and guidance for improvement. Review key findings and results during a facilitated discussion. As outcome of assessment project we deliver aligned with client, clearly defined and approved security strategy that will help
organization to achieve its business goals and meet security compliance and best practices.



UNDER DEFENSE

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

UD Observations	UD Recommendations
ID.AM-1: HPE IMC is utilized for inventory of network devices, (e.g., HP switches) both for internal and external devices; Lansweeper is utilized as a main asset management solution. The tool provides inventory of all workstations, ESXI servers, routers, switches, monitors, printers, NAS devices. Inventory specifications include: manufacturer, device type, model.	Document and implement a formal Asset Management Policy that establishes assets inventory and methods of inventory whether it is conducted manually or with help of automatic tools. For each asset organization must document sufficient information to identify the asset, its physical (or logical) location, information security classification.