UnderDefense
CyberSecurity solutions protecting your business

NIST Cybersecurity Framework Assessment for [Name of company]

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.

Respondent	**Position**

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 responsibilitie s 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.

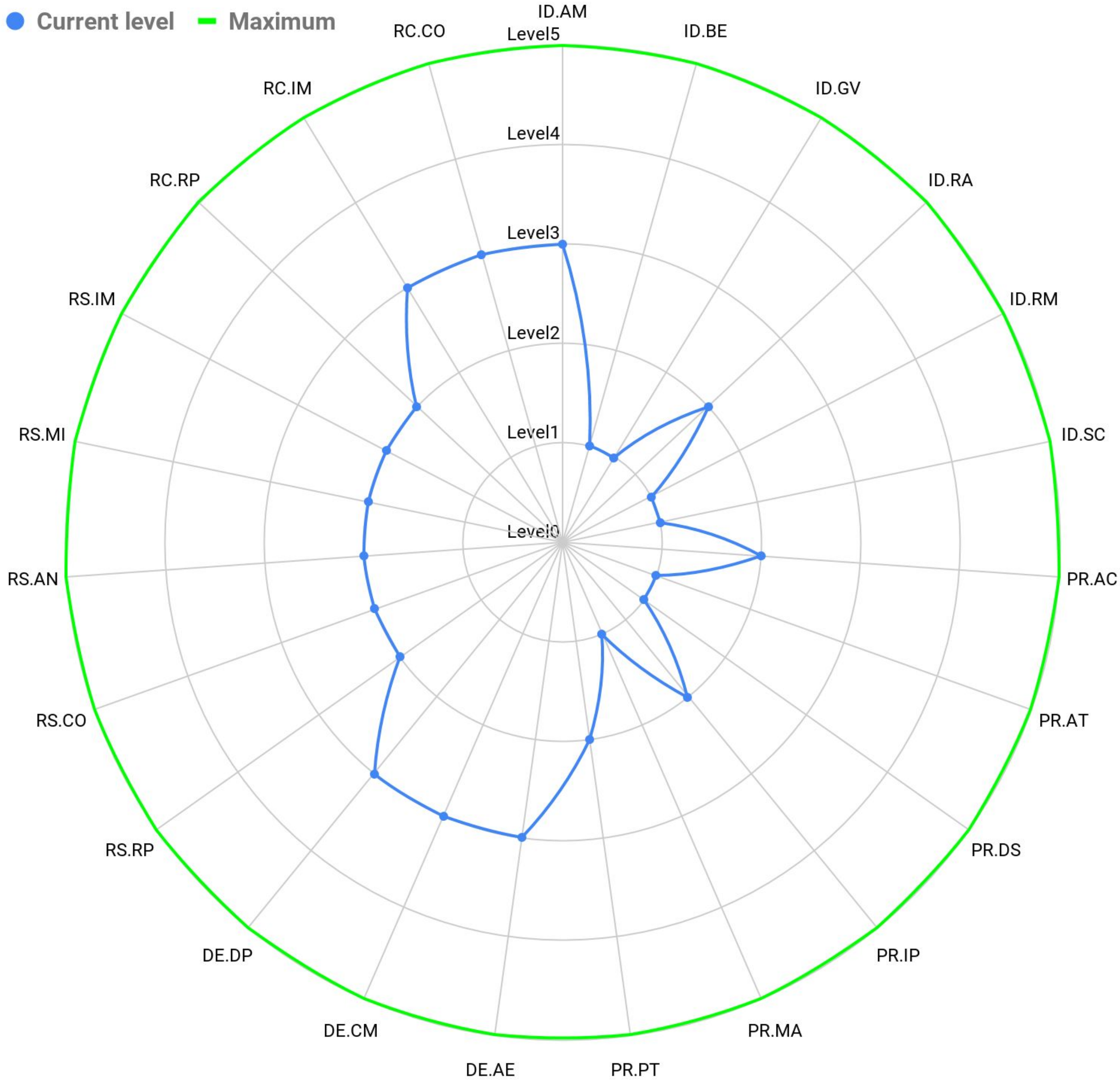


Figure 1. Graphical representation of each maturity level

RoadMap

(Green cells indicates that step was taken)

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
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	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
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.

ID.AM-2:	Pay attention to unauthorized software assets in Lansweeper. Define, document and implement procedure for handling unauthorized software. The software should be whether approved or eliminated by the administrator; Document and implement software baseline configurations for virtual machines which are run on employees laptops. Which software they should run and which they must not run in virtual machines. Potential malicious software that is run in virtual machines is not visible for Antivirus solutions;
ID.AM-3: We did not find evidence of the existence of documented procedures for how data should be transferred between all employees.	Document all connections within the organization, and between departments. All connections must be documented, authorized, and reviewed. Connection information includes, for example, the interface characteristics, data characteristics, ports, protocols, addresses, description of the data, security requirements, and the nature of the connection. Establish and document guidelines for electronic messaging usage which make users aware of what [*Name of company]* deems as acceptable and unacceptable use of its corporate messaging process. Consider following: https://www.securemessagingapps.com/ Create and implement Acceptable Use Policy, include these guidelines into the policy. Consider following: https://www.sans.org/security-resources/policies/general/doc/acceptable-use-policy
ID.AM-4: There are about 200 cloud servers on AWS, 5 on iWEB and OVH, couple Bare-metal cloud servers. Zabbix is functioning preferably for monitoring, there is just a list of cloud servers.	Finish up Service Catalogue creation. Describe procedures and all details related to cloud inventory in Asset management policy. Who is responsible for inventory, how inventory is done, etc.

Infrastructure Services Team is developing a registry (a.k.a Service Catalogue), where all cloud servers would be listed, divided into projects. Each server would have its owner.	
ID.AM-5: Organization's Information classification guidelines are described in Information Classification Policy. We found no formal procedures related to prioritization of organizational assets.	Develop and implement information classification basing on impact level classification. Information should be classified basing on its value. This means that relevant impact levels should be mapped to each of information classification levels. Classification guideline should take into account impact from loss of integrity, availability and confidentiality of the information. Implement formal procedures describing prioritization of organizational assets based on their importance to organizational systems. Prioritization means ranking your system's assets to help you decide how to allocate resources. Factors involved in prioritization include: How soon will you have to replace an asset? (is it remaining useful?) How important the asset is to the provision of production?(its impact on public health)? How important the asset is to the operation of the information systems (can other assets do the same job)?
ID.AM-6: Cybersecurity roles and responsibilities are established within Information Security Policy, Vulnerability Management, IT Security Incident Response policies.	Establish strict requirements that obligates each policy contain cybersecurity roles. Roles have to be widely communicated to all relevant parties. Third-party providers are required to notify the organization of any personnel transition (including transfers or terminations) involving personnel with physical or logical access to the production system components.
Maturity Level observed by UD	LEVEL 3 - ESTABLISHED
Documents reviewed	● List of information classification categories.docx ● Vulnerability Management.doc ● IT security incident response team composition (document).doc

Business Environment (ID.BE)	
Short description	The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
Subcategories	**ID.BE-1:** The organization’s role in the supply chain is identified and communicated **ID.BE-2:** The organization’s place in critical infrastructure and its industry sector is identified and communicated **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established **ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)

UD Observations	UD Recommendations
ID.BE-1: The organization acts both as a software, service supplier and as a buyer; Head of Partners Department responsible for relationships with IT vendors, purchasing software and hardware solutions, hardware repair operations, software licence management; The purchase decision is based on 6 requirements/criterias; Trade of analysis is made for expensive solutions, top management may be involved; Documentation of legal agreements such as contracts with vendors, leases and licensing agreements is not implemented; *[Name of company]* utilize third-party software for delivering service. Compliance department responsible for compliance of software usage. If possible, software EULA will be reviewed before utilization. There are 5 categories of accepted software usage(Approved, Purchased, Denied, etc.). In some cases company may ask third-party vendor for permission to use software. The permission is informal, contractual agreements are not signed;	Define information security requirements to apply to product or service acquisition in addition to the general requirements for supplier relationships. For example, do supplier has licence for commercial activity, ISO 9000 certifications, etc? Apply requirements to each supplier.

ID.BE-2: : UD did not find formal statements, policies which would describe the organization’s place in critical infrastructure, its industry sector and how it is identified and communicated.	Define, document and communicate critical infrastructure and key resources relevant to the company’s production activity. Develop, document, and maintain a critical infrastructure and key resources protection plan.
ID.BE-3: UD did not find formal statements, policies which would describe priorities for organizational mission, objectives, and activities how it is established and communicated.	Establish and communicate priorities for production activities, missions, objectives, with consideration for security. Make sure cybersecurity priorities align with business needs and priorities.
ID.BE-4: Secondary commercial power supply is implemented. Long-term alternate power supply provided by UPS and/or diesel generators.	Write down procedures describing all alternate power support services. Establish regular ability and capacity testing of alternative support services.
ID.BE-5: Critical infrastructure services concentrated in the main office and in data center. Data center provides continuity of daily operation for critical system; Cloud infrastructure is designed in such a way that one part of it supports another which falls.	Conduct contingency planning for the continuance of essential production functions and services with little or no loss of operational continuity, and sustain that continuity until full system restoration. Communicate that planning to all relevant parties, so that they aware of their roles, responsibilities and procedures.
Maturity Level observed by UD	LEVEL 1 - PERFORMED
Documents reviewed	N/A

Governance (ID.GV)	
Short description	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
Subcategories	**ID.GV-1:** Organizational cybersecurity policy is established and communicated **ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed **ID.GV-4:** Governance and risk management processes address cybersecurity risks
UD Observations	UD Recommendations
ID.GV-1: The organization has developed Information Security Policy that defines objectives and principles of information security. The Policy also defines the roles and responsibilities of all relevant representatives involved into information security activities; The company has only part of an ISMS (Information Security Management System) which includes the following policies: 1. Vulnerability Management Policy 2. Data Processing Agreement 3. Information Classification Policy 4. Data Protection Impact Assessment Methodology 5. Access management policy 6. Dismissal Process 7. IT Security Incident Response 8. Antivirus Policy 9. Incident Management 10. Password Protection Policy Data Protection Impact Assessment refers to to non-existent document - Data Protection Impact Assessment Questionnaire.	The best practice is to divide security rules into several policies like Access Control Policy, Classification Policy, Backup Policy, Acceptable Use Policy, etc. – this way such policies will be shorter (and therefore easier to read and understand), and easier to maintain (e.g. system administrator will be responsible for Backup Policy, while security manager will be responsible for Classification Policy); Establish and communicate existing cybersecurity policies to all relevant parties. Policies must include, for example, the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance. It also reflects coordination among organizational entities responsible for the different aspects of security (i.e., technical, physical, personnel, cyber-physical, access control, media protection, vulnerability management, maintenance, monitoring), and covers the full life cycle of the production system; Unify all cybersecurity policies into higher level entity - namely ISMS (Information Security Management System).

	Document ISMS scope including the list of the areas, locations, assets, and technologies of the organization. Document all exclusions from ISMS scope (e.g., sales representative offices, software developed by client-facing project teams, etc.), and justification for exclusion from the scope. Review and re-approve ISMS scope document with management annually or in cases if significant changes to the environment occur outside of the annual review cycle (e.g. regulatory changes, the inclusion of new locations, etc.).
ID.GV-2: Cybersecurity roles and responsibilities are coordinated within Information Security Policy, Vulnerability Management, IT Security Incident Response policies. Cybersecurity roles are not coordinated and aligned with internal roles and external partners. Not all managers engaged in driving security within the business. QA Team Lead noticed lack of Security Expert who would help the team to establish Security Testing program.	Describe and establish cybersecurity roles, responsibilities and procedures related to internal roles within whole organization and external partners. Develop, document and implement Security Testing procedures within general testing, define roles and responsibilities.
ID.GV-3: The company adheres to legal compliance with EU and US legislation. The company provides individuals the right to obtain a copy of their personal data. The right to data portability is fulfilled, personal data is provided using open formats such as JSON; Director of Engineering noted that *[Name of company]* functionality provides customer's PII that includes only name, surname billing information. At the same time *[Name of company]* (Figure 3) allowed to download multiple customers PII within one archive (name, surname, email, address, IP, billing data, postal code, geographical data and photos). The bug can be result of poor test cases, lack of communication. *[Name of company]* is a controller of PII(personal identifiable information). Google and Amazon are the processors of PII. Data Processing Agreement was concluded	Make sure your testing procedures contain enough Unit Tests, Service Tests, User Interface Tests, tests with different granularity; Make sure that requirements related to GDPR compliance, legal and regulatory requirements affecting the production operations regarding cybersecurity are understood, managed and widely communicated between all relevant parties(QA, engineering, marketing); As per the General Data Protection Regulation (GDPR) any personal data must not be kept any longer than it is necessary for the purpose for which the personal data is processed.

between companies (controller and processor) The organization's developed Classification Matrix of Personal Data. The Matrix is represented in form of Excel tables that mapped on business processes in Business Studio. The Matrix defines Personal Identifiable Information that should be protected; The company stores PII during five years; According to Privacy Policy individuals has right to: - Update account information; - Choose to opt-in or opt-out of *[Name of company]* marketing communications; - Access data that has been collected about you by *[Name of company]*; - Restrict processing of personal data; - Deactivate your *[Name of company]* Account or delete the personal information The company does not store the client CC (credit card) numbers; Mobile numbers are encrypted so that customer support agents cannot see them. The company do not render services to clients whose age has not reached 16 years of age.	
ID.GV-4: The organization did not establish risk management process addressing cybersecurity risks.	Establish Risk Management Process; Create Risk Management Framework document that would contain risk factors: threats, vulnerabilities, impacts, likelihoods, risk levels matrix. These factors are important for the organization to document prior to conducting risk assessment because the assessment rely upon well-defined attributes of threats, vulnerabilities, impact, and other risk factors to effectively determine risk. 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.
Maturity Level observed by UD	LEVEL 1 – PERFORMED
Documents reviewed	● Data protection impact assessment. (document).docx ● GDPR part in QSD.docx

Risk Assessment (ID.RA)

Short description	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
Subcategories	**ID.RA-1:** Asset vulnerabilities are identified and documented **ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources **ID.RA-3:** Threats, both internal and external, are identified and documented **ID.RA-4:** Potential business impacts and likelihoods are identified **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk **ID.RA-6:** Risk responses are identified and prioritized

UD Observations	UD Recommendations
ID.RA-1: The organization has implemented policy which defines roles, responsibilities and procedures within Vulnerability Management Process. At the moment, organization has implemented Tenable.IO and Nessus Professional which is used for scanning staging, development, production environments and internal infrastructure. Web Application scanning. There are approximately 250 scanned assets.	Define scope of Tenable.IO and Nessus Professional operation(IP ranges, internal users accounts, Amazon VPC ranges) within your Vulnerability Management Process.
ID.RA-2: Cyber threat intelligence is not received on regular basis. We did not find evidence of the existence of related agreements with any third-party companies or sources.	Consider possibility to receive cyber threat intelligence. Threat intelligence feeds take security data from vendors, analysts and other sources about threats and unusual activity happening all around the world. Malicious IP addresses, domains, file hashes and other data stream in constantly from external parties.
ID.RA-3: External threats are identified and documented within Tenable.IO and Nessus Professional reports. Internal threats are not identified due to the absence of related procedures. Regular scanning of internal infrastructure (ESXi servers, users laptops: Windows OS, Mac OS, GNU/Linux) is not established.	Conduct Vulnerability Scanning against internal environment(ESXi servers, users laptops: Windows OS, Mac OS, GNU/Linux) Conduct Penetration test and remediation testing of both infrastructure and web applications annually.

ID.RA-4: Due to absence of formal risk assessment process potential business impacts and likelihoods are not identified.	Develop potential business impacts and likelihoods ranges within risk assessment process.
ID.RA-5: Formal risk assessment process was not implemented.	Define, document and implement formal risk assessment process.
ID.RA-6: Due to absence of formal risk assessment process risk responses are not identified.	Identify and prioritize risk responses within risk assessment process.
Maturity Level observed by UD	LEVEL 2 - MANAGED
Documents reviewed	N/A

Risk Management Strategy (ID.RM)	
Short description	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions
Subcategories	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed **ID.RM-3:** The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

UD Observations	UD Recommendations
ID.RM-1: The organization has not developed and documented a comprehensive Risk Management Framework that would describe all steps and relevant methods required to be carried out in terms of risk assessment process, including: - Asset Identification; - Threat Identification; - Vulnerability Identification; - Control Analysis; - Likelihood Determination; - Impact Analysis; - Risk Determination; - Control Recommendations; - Results Documentation.	Establish Risk Management Process; Create Risk Management Framework document that would contain risk factors: threats, vulnerabilities, impacts, likelihoods, risk levels matrix. These factors are important for the organization to document prior to conducting risk assessment because the assessment rely upon well-defined attributes of threats, vulnerabilities, impact, and other risk factors to effectively determine risk. 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.
ID.RM-2: Due to absence risk management process risk tolerance is not determined.	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.
ID.RM-3: Due to absence of risk tolerance it cannot be informed by its role in critical infrastructure.	To maximize the benefit of risk assessments, the organization should establish policies, procedures, and implementing mechanisms to ensure that the information produced

	during such assessments is effectively communicated and shared across all risk management tiers.
Maturity Level observed by UD	LEVEL 1 – PERFORMED
Documents reviewed	N/A

Supply Chain Risk Management (ID.SC)

Short description	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
Subcategories	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders **ID.SC-2:** Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan. **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers

UD Observations	UD Recommendations
ID.SC-1: Cyber Supply Chain Risk Management processes are not established.	Establish Supply Chain Risk Management. Integrate SCRM into Risk Management Process. Risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented. Consider following: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf
ID.SC-2: Suppliers and third party partners of information systems, components are identified within different departments:	Create a list of all suppliers and third party partners. The list will serve as an input for Supply Chain Risk Management.
ID.SC-3: Contractual agreements established only with part of suppliers and third-party partners Partners Department has not documentation of legal agreements such as contracts with vendors, leases and licensing agreements; *[Name of company]* utilize third-party software for delivering service. In some cases	Consider absence of contractual agreements with certain suppliers as a risk. Establish documentation phase of a third-party relationship for allocating risk through negotiations and contracts. Establish the project scope, business objectives and identify the metrics and processes for monitoring and evaluating whether the

company may ask third-party vendor for permission to use software. The permission is informal, contractual agreements or NDA are not signed.	third-party supplier/ partner is meeting those objectives and appropriately managing risk. Create threat scenarios(Figure 4) for third-party suppliers to understand whether they meet the objectives of an organization's cybersecurity program. Upon results of threat scenarios the organization identify reliability of third-party software suppliers, risk of c ooperation with them, importance of signing contractual agreements, etc.
ID.SC-4: We did not find evidence of the existence of formal policy describing procedures of assessment or evaluation of suppliers and third-party partners. If possible, *[Name of company]* Compliance Department will review Privacy Policy or software EULA before utilization third-party solutions.	Create and establish a formal policy that would describe quality control measures, procedures need to be taken to ensure that third-party, vendors, suppliers guarantee that their products and services are satisfactory for organization's business requirements. Define roles and responsibilities; Create a list of questions that covers your organization's key risks areas, in addition to standard questions about product quality and operations. The list should include both local regulatory requirements, specific requirements applicable in the markets where you want to sell third parties' products and international compliance laws. Trade regulations and commerce laws are always changing so you need to periodically review statutory and other local requirements to make sure the terms of your contracts comply with current international and local laws, rules and regulations.
ID.SC-5: We did not find evidence of the existence of formal procedures describing response, recovery planning and testing 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.
Maturity Level observed by UD	LEVEL 1 - PERFORMED
Documents reviewed	N/A

PROTECT (PR) Function

Identity Management, Authentication and Access Control (PR.AC)	
Short description	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
Subcategories	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes **PR.AC-2:** Physical access to assets is managed and protected **PR.AC-3:** Remote access is managed **PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties **PR.AC-5:** Network integrity is protected (e.g., network segregation, network segmentation) **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi- factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

UD Observations	UD Recommendations
PR.AC-1: Access Control Policy defines requirements, roles, responsibilities and process of managing logical access to [*Name of company]* information systems; Access management works as Jira workflow; We did not find evidence of the existence of formal process of review access rights; Desktop Team Lead noted issue with Apple Developer ID Application Certificates, too many people have access to certificates; Web Services Team Lead noted issue with auto login links which are never expired; Access to logs distributed logically between AD groups.	Define, document and implement process for asset owners to review access rights to their assets on a regular basis. Review and verify process with all relevant parties. Remove Apple Developer ID Application Certificates from gitlab repositories to eliminate high security risks. Review architecture of CI/CD so that there are no risks of Certificates leakage. Include procedures describing Certificates issuance in Access Control Policy. Consider following: https://aws.amazon.com/blogs/aws/aws-secrets-manager-store-distribute-and-rotate-credentials-securely/ Resolve the issue with auto login links. Define certain expiration time. Ensure that all IAM users which are not used for 90 Days are inactivated or deleted

	UD recommend to rotate aws keys every 90 days. Consider following: https://aws.amazon.com/blogs/security/how-to-rotate-access-keys-for-iam-users/
PR.AC-2: Formal policy describing physical access control procedures is not implemented. Physical access control is implemented, RFID cards are issued to each employee. Electronic logging of each employee is implemented A physical log book for guests is maintained by the receptionist; Guest visitors must provide following information: name, surname, signature, entry and departure times. Guest cards provide with limited access to physical facilities; There are restricted areas: warehouse with equipment, parking, server rooms, accounting department. Only five people have access to the server room (logging is implemented).	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;
PR.AC-3: Remote Work Rules document describe procedures of remote work and remote access to information systems; Access to corporate network is provided by VPN. The organization is currently transferring from L2TP/IPsec to OpenVPN solution; Access to information and application systems such as Jira, Confluence, Salesforce, GitLab, etc. provided by single sign-on (SSO) of a self-hosted Active Directory Federation Services (ADFS) server.	Turn Remote Work Rules into formal policy (e.g Remote Work or Teleworking Policy), define roles and responsibilities. Finish up with transition from L2TP/IPsec to OpenVPN; Allow remote access only through approved and managed access points; Monitor 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.
PR.AC-4: Separation of duties is realized within MS Active Directory Group Policy Objects. There are Privileged Accounts and Groups in Active Directory; Access to corporate services mostly provided by domain authorization and SSO authentication. IT Security Team noted that there are services contain PII with local authorization, which harder to track and revoke access in timely manner; LastPass password manager is used in IT Infrastructure department.	Consider high risks from Ping Castle reports related to admin accounts (suspicious account(s) used in administrator activities, Administrator Account can be delegated, etc.) Take appropriate actions to mitigate these risks, consider advised solutions from the report. Describe job responsibilities for each employee in the organization in order to have possibilities for analyses all unauthorized actions. Implement specific restrictions. Specific restrictions can include, for example,

AWS IAM roles are not issued considering least privileges principle. The Scout2 report shows that IAM role (firs) have a policies that allow full administrative privileges. If the role is compromised by an attacker it can result in a full takeover of AWS account; AWS IAM roles don't include Support IAM Role.	restricting usage to certain days of the week, time of day, or specific durations of time. Privileged user access through non-local connections to the production system is restricted and managed. Based on open sources, only 10% of business services support the SAML protocol (used for SSO), while the remaining 90% of business applications/services only support password-based authentication. Password managers can cover both business and personal accounts so all of the sensitive data can be kept there; Conduct trade-off analysis for password managers software. Create and implement procedures which will describe how to use password managers for all employees. These procedures should include how to share passwords between a certain group of people, admin controls to view and manage permissions to each shared password, how to manage passwords in the dismissal process etc. Create an IAM Role to allow authorized users to manage incidents with AWS Support. Consider following: https://d1.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf
PR.AC-5: Network segmentation is done via Virtual Local Area Networks, each department has its own VLAN or divided into several VLAN's based on AD GPO's. Network segregation provided by WatchGuard Firebox firewalls, IDS, IPS, application control is enabled. No formal procedures for rules reviews and actualisation.	Document formal procedures describing review and actualisation of firewall configurations, IDS, IPS rules at least once per quartal. Define roles and responsibilities.
PR.AC-6: IT Security Team conducts quarterly audit for revealing residual ex-employees accounts.	Consider high risks from Ping Castle report related to Inactive objects in Active Directory Take appropriate actions to mitigate these risks, consider advised solutions from the report.
PR.AC-7: Users devices are authenticated and connected via WPA2-Enterprise with 802.1x authentication. Certificate Authority is set up;	Create and implement procedures which will describe authentication for all devices, users, and assets within the organization. Shift 2-Step Verification solution from text messages (SMS) to Authenticator app. Modern

The organization utilize text messages (SMS) as 2-Step Verification in G Suite; Considering prowler_*[Name of company]*-stage report UD discovered next findings: - Not all AWS IAM users have enabled MFA; - AWS access keys are not rotated in over 90 days; - The IAM Password Policy is not conformant to best practice.	hacker's techniques allow them to bypass SMS 2-Step Verification.Consider following: https://breakdev.org/evilginx-advanced-phishing-with-two-factor-authentication-bypass/ Enable Multi Factor Authentication for all AWS IAM users; UD strongly recommend using passphrases as a password for all users.
Maturity Level observed by UD	LEVEL 2 -MANAGED
Documents reviewed	Access management policy.docx Access management policy (process in Jira).doc Ping Castle report. Ping Castle report. Remote work rules.docx

Awareness and Training (PR.AT)	
Short description	The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cyber security related duties and responsibilities consistent with related policies, procedures, and agreements.
Subcategories	**PR.AT-1:** All users are informed and trained **PR.AT-2:** Privileged users understand their roles and responsibilities **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities **PR.AT-4:** Senior executives understand their roles and responsibilities **PR.AT-5:** Physical and cybersecurity personnel understand their roles and responsibilities
UD Observations	UD Recommendations
PR.AT-1: Formal Security Awareness Policy describing roles, responsibilities and procedures of security awareness is not implemented; IT Security Team conducted Security Awareness for *[Name of company]* staff. Security awareness presentation contains very few cybersecurity topics;	Define, document and implement Security Awareness and Training Policy that defines scope, procedures, topics, roles and responsibilities in terms of Security Awareness and Training Program. **Awareness is not training.** The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. **Training** strives to produce relevant and needed security skills and competencies. Consider the following scheme(Figure 5) when deciding whether the department should go through Security Awareness or Training. Implement an information security workforce development and improvement programs which include, for example: defining the knowledge and skill levels needed to perform information security duties and tasks; Use anecdotes from actual information security incidents in user awareness training as examples of what could happen, how to respond to such incidents and how to avoid them in the future.

	Consider following: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf
PR.AT-2: Due to the absence of formal Security Awareness and Training Policy, specific cybersecurity awareness and training procedures for privileged users (e.g. developers) are not established.	Establish specific cybersecurity awareness and training procedures for privileged users (e.g. developers) describing acceptable and unacceptable activities at workplace.
PR.AT-3: Due to the absence of formal Security Awareness and Training Policy, roles and responsibilities of third-party stakeholders (e.g., suppliers, customers, partners) are not defined.	Define cybersecurity roles and responsibilities within Security Awareness and Training Policy.
PR.AT-4: Cybersecurity roles and responsibilities are established only in Information Security Policy, Vulnerability Management, IT Security Incident Response policies.	
PR.AT-5: Due to the absence of formal Security Awareness and Training Policy, cybersecurity roles and responsibilities are not defined.	
Maturity Level observed by UD	LEVEL 1 - PERFORMED
Documents reviewed	Security awareness presentation.pptx

Data Security (PR.DS)	
Short description	Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.
Subcategories	**PR.DS-1:** Data-at-rest is protected **PR.DS-2:** Data-in-transit is protected **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition **PR.DS-4:** Adequate capacity to ensure availability is maintained **PR.DS-5:** Protections against data leaks are implemented **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity **PR.DS-7:** The development and testing environment(s) are separate from the production environment **PR.DS-8:** Integrity checking mechanisms are used to verify hardware integrity
UD Observations	UD Recommendations
PR.DS-1: Due to the absence of formal risk assessment process, strategy to protect the confidentiality, integrity, and availability of information is not established; One of the main organization’s objective is the protection of customer’s PII. Considering Prowler report UD noticed: - Unencrypted EBS Volumes; - SQS queues haven’t Server Side Encryption enabled.	Create and implement procedures which describe how to encrypt all data related to PII within all AWS infrastructure.
PR.DS-2: The organization doesn’t have documented procedures for how data should be transferred between all employees. Considering the Scout2 report UD found that AWS S3 buckets allows clear text (HTTP) communication.	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 correct obfuscate data before transfer or how to choose a protected way for transferring data. Conduct trade-off analysis of data protection solutions with policies that enable user prompting, blocking, or automatic encryption for sensitive data in transit, such as when files are attached to an email message or moved to cloud storage, removable drives, or transferred elsewhere.

	Ensure your Information Classification Policy requires classifying all company data, no matter where it resides, in order to ensure that the appropriate data protection measures are applied while data remains at rest and triggered when data is accessed, used, or transferred. Implement SSL/TLS encryption for all HTTP transactions.
PR.DS-3: Removal, transfer and disposal of assets managed within several procedures: Access Control Policy, Dismissal Process.	Document roles, responsibilities and procedures within Dismissal Process. Add procedures that describe the secure formatting of data from each media drive.
PR.DS-4: We did not find evidence of the existence of implemented capacity monitoring to ensure availability is maintained within whole organization. Duty Team monitor availability of AWS infrastructure.	Create and implement procedures which will describe how to monitor and maintain a capacity and availability of both internal and external infrastructure. Conduct regular performance and load tests for both internal and external infrastructure.
PR.DS-5: The organization did not implement DLP solution; The organization conducted audit of organization’s Google Docs to manually reveal and delete PII; We did not find evidence of the existence of documented procedures defining Full Disk Encryption(FDE) utilization.	Consider creation of organizational units within your G Suite: https://support.google.com/a/answer/4352075?hl=en Confine file sharing for specific organizational units : https://support.google.com/a/answer/7492096?hl=en Conduct trade-off analysis of DLP solutions to implement protections against data leaks. Create and document procedures defining correct equipment maintenance outside the organization's premises. Confidential information must be protected with Full Disk Encryption. You can include these procedures into Acceptable Usage Policy. Consider following: https://www.sans.org/security-resources/policies/general/doc/acceptable-use-policy
PR.DS-6: Software integrity is provided by Lansweeper inventory tool, scope - users workstations, ESXI servers, routers, switches, monitors, printers, NAS devices. Information integrity is covered by default Google Docs features (automatic changes saving, Version history).	Pay attention to unauthorized software assets in Lansweeper. Define, document and implement procedure for handling unauthorized software. The software should be whether approved or eliminated by the administrator;

PR.DS-7: QA Team Lead noticed lack of fully functional testing environment, some test cases can be performed on production environment.	Implement fully functional testing environments, so that test cases can be performed without afraid to cause damage to production environment.
PR.DS-8: Hardware integrity is provided by Lansweeper inventory tool, scope - users workstations, ESXI servers, routers, switches, monitors, printers, NAS devices.	Conduct risk assessment on importance of monitoring hardware integrity. Based on results of risk assessment decide to what extent organization should monitor hardware integrity. Conduct trade-off analysis of possible solutions to monitor hardware integrity.
Maturity Level observed by UD	LEVEL 1 - PERFORMED
Documents reviewed	Access management policy.docx Dismissal process (document).doc

Information Protection Processes and Procedures (PR.IP)	
Short description	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
Subcategories	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) **PR.IP-2:** A System Development Life Cycle to manage systems is implemented **PR.IP-3:** Configuration change control processes are in place **PR.IP-4:** Backups of information are conducted, maintained, and tested **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met **PR.IP-6:** Data is destroyed according to policy **PR.IP-7:** Protection processes are improved **PR.IP-8:** Effectiveness of protection technologies is shared **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed **PR.IP-10:** Response and recovery plans are tested **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) **PR.IP-12:** A vulnerability management plan is developed and implemented

UD Observations	UD Recommendations
PR.IP-1: IT infrastructure department tried to implement software whitelist within whole organization, but it didn't bring results due to privileged users. Software whitelist works only for several departments (e.g. HR, Accountants)	Develop, document, and maintain a baseline configurations for the organization. Baseline configurations include for example, information about infrastructure of organization components (e.g. software license information, software version numbers, operating systems, patch information on operating systems and applications, network topology) and the logical placement of those components within the infrastructure; Configure the production to provide only essential capabilities;

	Review and update the baseline configuration and disable unnecessary capabilities; Focus on securing the highest privilege accounts and groups. You should do so because they can be leveraged by attackers to compromise and even destroy your Active Directory installation. Consider following: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory
PR.IP-2: Apple Security Framework is utilized during development of desktop applications https://developer.apple.com/documentation/security Practises for establishing a secure configuration of microservices(Amazon EKS) is not considered.	Consider use of Secure Code Development practises where appropriate. Create and implement Software Development Life Cycle (SDLC) Policy that would describe the requirements for developing and/or implementing new software and systems.
PR.IP-3: Change Management procedures described are developed within 'IT change management' and 'How to handle new data processing' documents and instructions. Data Handling Change management block diagram describes schematically change management procedures.	Add next procedures to Change Management related documents. Procedures should describe how to: - Conduct security impact analysis in connection with change control reviews. - Conduct security impact analysis in a separate test environment before implementation into an operational environment for planned changes to the production. - Review and authorize proposed configuration-controlled changes prior to implementing them on the production environment. Consider unifying all Change Management related procedures into one policy.
PR.IP-4: Backups of internal infrastructure items (Domain controllers, NPS server, gitlab, jenkins, etc.) are made by bareos and windows backup services; Backups of external(cloud) infrastructure are stored on EBS (Elastic block storage).	Create and implement Backup Policy which will describe backup procedures, retention periods, types of backups, scope, roles and responsibilities.

Backups of logs are stored on S3, backups are made once per day(24 hours); The organization uses Snapshots to backup databases.	
PR.IP-5: Secondary commercial power supply is implemented. Long-term alternate power supply provided by UPS and/or diesel generators.	Define, implement, and enforce policy and regulations regarding emergency and safety systems, fire protection systems, and environment controls.
PR.IP-6: Data is destroyed according to formal policy. The policy covers data destruction procedures, roles and responsibilities.	Ensure that organization system data is destroyed according to policy. Implement regular testing of effectiveness of technical data destruction mechanisms, how they are measured and evaluated.
PR.IP-7: We found no evidence of existence procedures which allows the organization to learn from information security incidents and reduce the impact/probability of future events both in 'IT security incident response team composition (document).doc' and 'Incident management (business process, document).docx'	Implement The Follow-up Phase within your Incident Response policies that would represent the review of the Security Incident to look for "lessons learned" and to determine whether the process that was followed could have been improved in any way. Security Events and Security Incidents should be reviewed after identification resolution to determine where response could be improved.
PR.IP-8: We found no evidence of existence formal procedures which describe how to share effectiveness of protection technologies.	Share information about security incidents and mitigation measures with designated sharing partners; Use automated mechanisms where feasible to assist in information collaboration.
PR.IP-9: The organization has developed and maintained response and recovery plans that identify essential functions for restoring internal IT infrastructure.	Plans must incorporate recovery objectives, restoration priorities, metrics, contingency roles, personnel assignments and contact information. Conduct regular (quarterly) review of Incident Response and Disaster Recovery plans to keep them up-to-date.
PR.IP-10: We did not find evidence of the existence of testing Incident Response and Disaster Recovery plans.	Consider testing of relevant plans, make records, evaluate effectiveness.
PR.IP-11: Personnel screening procedures conducted by Security Service. The Service makes request for Ministry of Internal Affairs to check whether candidate had convictions.	Define, document and implement Onboarding Policy. Include personnel screening procedures within the policy.

PR.IP-12: The organization has implemented roles, responsibilities and procedures within Vulnerability Management Process; A vulnerability management plan is not developed within the Vulnerability Management Process. We have found no evidence of the existence of formal Patch Management Policy	Define scope of Tenable.IO and Nessus Professional operation(IP ranges, internal users accounts, Amazon VPC ranges). Establish and maintain a process that allows continuous review of vulnerabilities, and defines strategies to mitigate them. Restrict access to privileged vulnerability data. Create, implement and continuously maintain Patch Management Policy. The policy must define downtime windows. Downtime window must be defined for each device and application system in order to apply the appropriate patches. This window has to be determined so that it provides minimal disruption to business activities relying on that device or application system. All patches must be downloaded from the relevant system vendor or other trusted source.
Maturity Level observed by UD	LEVEL 2 - MANAGED
Documents reviewed	Vulnerability+Management.doc IT change management.docx Disaster recovery plan.docx IT security incident response team composition (document).doc Incident management (business process, document).docx Data protection impact assessment. (document).docx How to handle a data breach.docx Data Handling Change management.pdf IT change management.docx How to handle new data processing.docx

Maintenance (PR.MA)

Short description	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
Subcategories	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

UD Observations	UD Recommendations
PR.MA-1: IT Infrastructure Team and Partners Department are responsible for maintenance of equipment.	Document and communicate procedures of maintenance and repairs to all relevant stakeholders. For example, to prevent data leakage check whether full disk encryption is enabled or hard drive is removed before send laptop to repair service.
PR.MA-2: We did not find evidence of the existence of formal procedures which describe remote maintenance of organizational assets in a manner that prevents unauthorized access.	Establish, implement and communicate formal procedures which would describe how the organization: - Approves and monitors nonlocal maintenance and diagnostic activities; - Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; - Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; - Maintains records for nonlocal maintenance and diagnostic activities; - Terminates session and network connections when nonlocal maintenance is completed. Unify procedures into Remote Maintenance Policy or include them into Acceptable Use Policy.https://www.sans.org/security-resources/policies/general/doc/acceptable-use-policy

Maturity Level observed by UD	LEVEL 1 – PERFORMED
Documents reviewed	N/A

Protective Technology (PR.PT)	
Short description	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Subcategories	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy **PR.PT-2:** Removable media is protected and its use restricted according to policy **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities **PR.PT-4:** Communications and control networks are protected **PR.PT-5:** Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations

UD Observations	UD Recommendations
PR.PT-1: Log records are collected from AWS infrastructure. Log collection provided by Rsyslog. Graylog and ELK log management solutions are utilized primarily for availability Considering Prowler and Scout2 reports: - AWS CloudTrail is not enabled in order to conduct governance, compliance, operational auditing, and risk auditing of AWS account; - Flow Logging on AWS VPC is disabled; - CloudWatch doesn't make groups log metrics; - Logging on CloudFront distributions is not enabled; - Server access logging on S3 buckets is not enabled.	Create and implement a policy which will describe how to containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or organizational components associated with the event. Use CloudTrail in order to log, continuously monitor, and retain account activity related to actions across AWS infrastructure; Enable VPC Flow Logging in order to capture information about the IP traffic going to and from network interfaces in your VPC; Enable and configure CloudWatch groups Consider following: https://www.cloudconformity.com/conformity-rules/CloudWatchLogs/ Enable CloudFront distributions logging; Enable S3 buckets server access logging. Consider following: https://d1.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf

PR.PT-2: USB ports are locked using AD policies only in all *[Name of company]* offices.	Create and implement a policy which would describe how to protect and control portable storage devices containing critical data while in transit and in storage. Scan all portable storage devices for malicious content before they are used within the organization. Consider to restrict the use of portable storage devices within *[Name of company]* departments where appropriate.
PR.PT-3: Director of Engineering noted that developers have direct access to production infrastructure.	Ensure criteria used for granting access privileges is based on the principle of "least privilege" whereby authorized users will only be granted access to information system and network domains which are necessary for them to carry out the responsibilities of their company role or function. Relying on CI/CD best practises, developers are not expected to be experts at operations concerns. Assign one Application Operator who would have permissions to manage continuous delivery process for apps. Deny collective decision-making in the process of a release. Follow least functionality principle. Document procedures within Access Control Policy.
PR.PT-4: Considering Prowler report UD found that: - Default security group of every VPC doesn't restrict all traffic; - Two RDS instances are set as Publicly Accessible.	Take appropriate actions to eliminate non-conformities from Prowler report: - Disallow 0.0.0.0 IN or OUT traffic in all Regions, if it's doesn't interferers business goals; - Ensure that there are no Public Accessible RDS instances.
PR.PT-5: If there is an infrastructure failure, IT Infrastructure Team will manually replace broken item within minutes.	Test redundant information systems to ensure the failover from one component to another component works as intended.
Maturity Level observed by UD	LEVEL 2 - MANAGED
Documents reviewed	prowler-stage.txt report-kt-admin-aws-scan.html Access management policy.docx

DETECT (DE) Function

Anomalies and Events (DE.AE)	
Short description	Anomalous activity is detected and the potential impact of events is understood.
Subcategories	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed **DE.AE-2:** Detected events are analyzed to understand attack targets and methods **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors **DE.AE-4:** Impact of events is determined **DE.AE-5:** Incident alert thresholds are established

UD Observations	UD Recommendations
DE.AE-1: We have found no evidence that baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems; We have found no evidence that baseline configurations are constantly monitored and managed. Hardware and software inventory(Lansweeper) refers to baseline configurations. IT Infrastructure team responsible for Lansweeper inventory tool so responsible for hardware and software integrity too. We found evidence of unauthorized software assets in Lansweeper. Duty Team primarily keeps watching on the availability of information systems and applications.	Implement automated mechanisms that help the organization maintain consistent baseline configurations for information systems include, for example: - hardware and software inventory tools, - configuration management tools, - network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system, current patch levels, etc. Consider to implement monitoring of baseline configurations by Duty Team. For example, monitoring of unauthorized software and hardware in Lansweeper.
DE.AE-2: IT Security Team is currently working on Windows Events Collection. Events should be collected and forwarded to log management solutions so that administrator can analyze suspicious events. Events should be collected from internal Windows Servers, Domain Controllers, etc. The process is on initial phase.	Finish up with the process set up, implement measurements, determine and document the effectiveness of the process.

DE.AE-3: Event data are not collected and correlated from multiple sources and sensors.	Consider implementing correlation rules within your log management solutions to automate threat detection and log analysis. Consider acquiring a SIEM solution. A correlation rule tells your SIEM system which sequences of events could be indicative of anomalies which may suggest security weaknesses or cyber attack. When "x" and "y" or "x" and "y" plus "z" happens, your administrators should be notified. It helps to insure the security and confidentiality of customer records and information and to protect against any anticipated threats or hazards to the security or integrity of such records. Consider following: https://www.sans.org/reading-room/whitepapers/auditing/successful-siem-log-management-strategies-audit-compliance-33528 Ensure that event data is compiled and correlated across the organization system using various sources such as event reports, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Integrate analysis of events where feasible with the analysis of vulnerability scanning information; performance data; production systems monitoring, and facility monitoring to further enhance the ability to identify inappropriate or unusual activity.
DE.AE-4: Impact of events is determined according to Priority Matrix. Each business metric is mapped on a trigger.	Test ability and effectiveness of Priority Matrix to measure the influence on the business on regular basis. Share effectiveness with relevant stakeholders.
DE.AE-5: Incident alert thresholds are established in Priority Matrix. Each priority has expected time to resolution(e.g,, 2 hours, 1 business day, etc.)	Monitor and optimize Expected time to resolution. For example if there a case when Blocker took 5 hours, make update to your Priority Matrix. Employ automated mechanisms where feasible to assist in the identification of security alert thresholds.
Maturity Level observed by UD	LEVEL 3 - ESTABLISHED
Documents reviewed	Duty assess service. (IT policy).png KTINF-PriorityMatrix-101218-1331-834.pdf

Security Continuous Monitoring (DE.CM)	
Short description	The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Subcategories	**DE.CM-1:** The network is monitored to detect potential cybersecurity events **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events **DE.CM-4:** Malicious code is detected **DE.CM-5:** Unauthorized mobile code is detected **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed **DE.CM-8:** Vulnerability scans are performed
UD Observations	**UD Recommendations**
DE.CM-1: Watchguard logs are forwarded and processed in Graylog log management solution. There are very few streams (for WatchGuard firewalls, Active Directory installation, WiFi access points).	Consider implementing correlation rules within your log management solutions to automate threat detection and log analysis. Consider acquiring a SIEM solution.
DE.CM-2: The physical environment is monitored with: - Video surveillance; - Electronic logging of RFID cards.	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;
DE.CM-3: Personnel activity is monitored with Lansweeper, it it keeps watching on hardware and software changes. Logs are not collected from users workstations. Lansweeper automatically retrieve software information for all network PCs as well. It also detect any hardware or software changes that occur with inventory items. Lansweeper is integrated into company's Active Directory.	Consider implementing correlation rules within your log management solutions to automate threat detection and log analysis. Consider acquiring a SIEM solution. SIEM solution involves installing forwarders on users workstation. Logs are forwarded from workstation to SIEM.

DE.CM-4: The organization decided to acquire Cylance as primary antivirus endpoint protection. ESET utilized as secondary antivirus solution, primarily for server machines.	Annually conduct trade-off analysis of antivirus solutions. Testing of antivirus endpoint protection must be conducted based on conventional criteria. Consider following: https://selabs.uk/download/enterprise/epp/2018/jul-sep-2018-enterprise.pdf
DE.CM-5: Apple Security Framework is utilized during development of desktop applications https://developer.apple.com/documentation/security	Create and implement a policy which will describe how to use Mobile Code Security. UD also recommend paying attention to secure code developing and secure data during all development process in the organization.
DE.CM-6: We have found no evidence weather external service provider activity is monitored to detect potential cybersecurity events.	Create and implement procedures that would describe how to: - conduct ongoing security status monitoring of external service provider activity; - detect attacks and indicators of potential attacks from external service providers; - monitor compliance of external providers with personnel security policies and procedures, and contract security requirements.
DE.CM-7: The physical environment is monitored with: - Video surveillance; - Electronic logging of RFID cards. Personnel activity is monitored with Lansweeper, it it keeps watching on hardware and software changes Logs are not collected from users workstations. Lansweeper automatically retrieve software information for all network PCs as well. It also detect any hardware or software changes that occur with inventory items. Lansweeper is integrated into company's Active Directory.	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; SIEM solution involves installing forwarders on users workstation. Logs are forwarded from workstation to SIEM.
DE.CM-8: Vulnerability scans are performed with Tenable.IO and Nessus vulnerability scaners; There are 167 Tenable.IO agents reguraly scan external infrastructure, primarily web applications.	Document and implement vulnerability management plan; Define scope of Tenable.IO and Nessus Professional operation(IP ranges, internal users accounts, Amazon VPC ranges) within your Vulnerability Management Process.

Maturity Level observed by UD	LEVEL 3 - ESTABLISHED
Documents reviewed	

Detection Processes (DE.DP)	
Short description	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
Subcategories	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability **DE.DP-2:** Detection activities comply with all applicable requirements **DE.DP-3:** Detection processes are tested **DE.DP-4:** Event detection information is communicated **DE.DP-5:** Detection processes are continuously improved
UD Observations	**UD Recommendations**
DE.DP-1: Roles and responsibilities for detection are defined to ensure accountability. Duty Team acts as a Tier 1, notify accountable process owners(developers) who are Tier 2.	Keep roles and responsibilities for Duty team up-to-date. Provide security training activities which would involve coordination across all organizational elements.
DE.DP-2: Duty Team noted that there are no formal procedures which obligate engineers/developers to configure monitoring of service with the Team before deploying service into production. Developer can bypass this process, Therefore Duty Team is not aware of services which should be monitored.	Define, document, implement and communicate procedures describing configuring monitoring of services before deploying into production
DE.DP-3: We have found no evidence weather detection processes are tested on regular basis.	Implement formal procedures which would describe how the organization: - Creates a process for ensuring that organizational plans for conducting security testing, monitoring activities and training associated with organizational information systems; - Ensures that detection testing is executed in a timely manner - Reviews detection testing and monitoring plans for consistency with the organizational risk strategy.
DE.DP-4: Duty Team noted that event detection information is communicated in relevant Jira workflow.	Ensure that event detection information is communicated to defined personnel; Update list of events which must be detected on regular basis. Event detection information includes for example, alerts on atypical account usage, unauthorized remote access, wireless connectivity, mobile device connection, altered configuration settings, contrasting system component inventory, use of maintenance tools and nonlocal

	maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, use of VoIP, and malware disclosure.
DE.DP-5: Detection processes are continuously improved. Continuous service improvement established within Vulnerability Management Process. IT Security Team attempts to cover 100% assets and eliminate vulnerabilities in 48 hours. Jira workflow synchronized with Kibana to monitor metrics; Duty Team Jira workflow synchronized with Kibana to gather productivity metrics, determine KPI, etc.)	Incorporate improvements derived from the monitoring, measurements, assessments, and lessons learned into detection process revisions. Ensure the security plan for the production system provides for the review, testing, and continual improvement of the security detection processes; Employ independent teams to assess the detection process; Try enrich your detection assessments including: - vulnerability scanning; - malicious user testing; - insider threat assessment; - performance/load testing;. - verification and validation testing.
Maturity Level observed by UD	LEVEL 3 - ESTABLISHED
Documents reviewed	N/A

RESPOND (RS) Function

Response Planning (RS.RP)	
Short description	Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
Subcategories	**RS.RP-1:** Response plan is executed during or after an incident
UD Observations	**UD Recommendations**
RS.RP-1: The organization has adopted policies which regulates roles, responsibilities and procedures in terms of the incident management process. Policies include Incident management, IT Security Incident Response processes. Duty Team implemented separate Incident Management and Problem Management processes.Response plans is executed during or after an incident.	Incident Response, Incident Management processes, plans, policies should include: - Roles and Responsibilities employees - Detection Phase - Analysis Phase - Containment Phase - Mitigation Phase - Eradication Phase - Recovery Phase - Post-Incident Activities Ensure above mentioned activities are executed during or after an incident; Implement Incident Handling Checklists within your Incident Management processes, plans and policies, so that each team will take the appropriate sequence of actions depending on the type of incident. For example, Generic Incident Handling Checklist for Uncategorized Incidents (Figure 6) for IT Security Incident Response process. Denial of Service Incident Handling Checklist(Figure 7) for Duty Team Incident Management process. For your information: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-61.pdf
Maturity Level observed by UD	LEVEL 2 - MANAGED
Documents reviewed	IT security incident response team composition (document).docx Incident management (business process, document).docx Problem+Management.png Problem+Management.doc Incident+management.doc Incident+management.png KTINF-Incidentmanagement-101218-1332-836.pdf

Communications (RS.CO)

Short description	Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Subcategories	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed **RS.CO-2:** Incidents are reported consistent with established criteria **RS.CO-3:** Information is shared consistent with response plans **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness

UD Observations	UD Recommendations
RS.CO-1: Roles described within general Incident Management Policy and IT Security Incident Response Policy. Order of operations described in block diagrams(Activities) within each policy. We have found no evidence of the existence of procedures describing personnel(mission/business owners, production system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.) roles and order of operations when a response is needed;	Ensure personnel understand objectives, restoration priorities, task sequences and assignment responsibilities for event or incident response. Communicate procedures relevant to event or incident response to all relevant parties. Update Incident Management and IT Security Incident Response policies on regular basis.
RS.CO-2: We have found no evidence of the existence of formal procedure which describes how and where the employees can report the incident.	Create Security Incident Response Report Form to support the reporting action and to help the person reporting to remember all necessary actions in case of an information security event. Consider following: https://bok.ahima.org/PdfView?oid=76732
RS.CO-3: IT Security Incident Response Policy contains a procedure that obligates Administrator to share: - name and IP of affected item. - suggested type of incident - date and time of incident - other relevant information.	Share cybersecurity incident information with relevant stakeholders per the response plan.

RS.CO-4: Coordination is provided by a block diagrams(Activities) located in both of Response Policies.	Coordinate cybersecurity incident response actions with all relevant stakeholders. Stakeholders for incident response include for example, mission/business owners, manufacturing system owners, integrators, vendors, human resources offices, physical and personnel security offices, legal departments, operations personnel, and procurement offices.
RS.CO-5: We did not find evidence of the existence of share information with external stakeholders in order to achieve broader cybersecurity awareness.	Share cybersecurity event information voluntarily, as appropriate, with industry security groups to achieve broader cybersecurity awareness. Based on risk assessment decide weather cooperation and information sharing with Cyber Police and CERT-UA are needed.
Maturity Level observed by UD	LEVEL 2 - MANAGED
Documents reviewed	IT security incident response team composition (document).docx Incident management (business process, document).docx

Analysis (RS.AN)

Short description	Analysis is conducted to ensure effective response and support recovery activities.
Subcategories	**RS.AN-1:** Notifications from detection systems are investigated **RS.AN-2:** The impact of the incident is understood **RS.AN-3:** Forensics are performed **RS.AN-4:** Incidents are categorized consistent with response plans **RS.AN-5:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

UD Observations	UD Recommendations
RS.AN-1: There are 3000 events collected from Cylance endpoint protection. IT Security Team started to analyze and categorize these events. The process on initial phase.	Create and document formal procedures of events investigation, define roles and responsibilities, implement metrics, determine effectiveness. Consider implementation of security orchestration solutions to automate decision making.
RS.AN-2: We have found no evidence of the existence of the formal procedures describing how the impact of the incident is understood.	Conduct quantitive and qualitive risks analysis of impacted assets. Correlate detected event information and incident responses with risk assessment outcomes to achieve perspective on incident impact across the organization.
RS.AN-3: We did not find evidence of the existence of formal forensics procedures.	Conduct forensic analysis on collected cybersecurity event information to determine root cause. Consider outsourcing on-demand audit reviews, analysis, and reporting for investigations of cybersecurity incidents.
RS.AN-4: According to IT Security Incident Response Policy incidents are categorized and classified into four categories: low, average, high, critical. We have found no severity categories within general Incident Management process.	Develop severity categories to assess cybersecurity incidents within each Incident Response plan, policy or process.
RS.AN-5: Bugcrowd - platform for security researchers to identify critical software vulnerabilities. The platform is listed as a third party partner of *[Name of company]*. We did not find evidence of the existence of information whether company has private bug bounty program on the platform.	Consider creation public or private bug bounty program so that it is possible to receive, analyze and respond to vulnerabilities disclosed to the organization.

Maturity Level observed by UD	LEVEL 2 - MANAGED
Documents reviewed	Incident management (business process, document).docx IT security incident response team composition (document).doc

Mitigation (RS.MI)	
Short description	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
Subcategories	**RS.MI-1:** Incidents are contained **RS.MI-2:** Incidents are mitigated **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks
UD Observations	**UD Recommendations**
RS.MI-1: We have found procedures which might describe containment of cybersecurity incidents. We have found no detailed description of Containment Phase.	Describe and include Containment Phase that limits the root cause of the Security Incident to prevent further damage or exposure. Containment Phase might include following steps: - Short-term Containment; - System Back-Up; - Long-term containment. Short-term Containment; basically the focus of this step is to limit the damage as soon as possible. Short-term containment can be as straightforward as isolating a network segment of infected workstations to taking down production servers that were hacked and having all traffic routed to failover servers; System Back-Up; it is necessary before wiping and reimaging any system to take a forensic image of the affected system(s); Long-term containment, which is essentially the step where the affected systems can be temporarily fix in order to allow them to continue to be used in production, if necessary, while rebuilding clean systems in the next phase; A good example of containment is disconnecting affected systems by either disconnect the affected system's network cable or powering down switches and/or routers to entire portions of the network to

	isolate compromised systems from those that have not been compromised. For your information: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
RS.MI-2: We have found procedures which might describe mitigation of cybersecurity incidents. We have found no detailed description of Mitigation Phase.	The organization must describe metrics which need to collect to mitigate future incidents. The organization should decide what incident data to collect based on reporting requirements and on the expected return on investment from the data (e.g., identifying a new threat and mitigating the related vulnerabilities before they can be exploited.) Possible metrics for incident-related data include: - Number of Incidents Handled; - Time Per Incident; - Objective Assessment of Each Incident; - Subjective Assessment of Each Incident. Consider following: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-61.pdf
RS.MI-3: Vulnerability Management Policy doesn't include procedures which describe how to mitigate newly vulnerability or document accepted risks.	Add to Vulnerability Management Policy procedures which will describe how to document and mitigate accepted risks and new vulnerabilities. For example, how to isolate vulnerable environment if there doesn't exist a solution to fix vulnerability and how to handle acceptable risks.
Maturity Level observed by UD	LEVEL 2 - MANAGED
Documents reviewed	IT security incident response team composition (document).doc Incident management (business process, document).docx Vulnerability+Management.doc

Improvements (RS.IM)	
Short description	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
Subcategories	**RS.IM-1:** Response plans incorporate lessons learned **RS.IM-2:** Response strategies are updated
UD Observations	**UD Recommendations**
RS.IM-1: There is Jira workflow created for corrective actions after incident response assessment; IT Security and IT Support Teams conduct weekly sync-up where current improvements are discussed; Security Assessment and Penetration Tests are conducted within this control.	Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; Write down lessons learned procedures into each incident response policy, procedure or process.
RS.IM-2: Response plan has been issued Sep 17 and since this time didn't be updated	Regularly update "Incident management" and "IT security incident response team composition" Updates may include, for example, responses to disruptions or failures, and predetermined procedures.
Maturity Level observed by UD	LEVEL 2 - MANAGED
Documents reviewed	IT security incident response team composition (document).docx Incident management (business process, document).docx

RECOVER (RC) Function

Recovery Planning (RC.RP)	
Short description	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
Subcategories	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident
UD Observations	**UD Recommendations**
RC.RP-1: There is a Disaster Recovery Plan document that describes recovery procedures of internal infrastructure. Roles are represented in tables. We have found no described responsibilities within the Plan; Disaster Recovery Plan is executed during or after a cybersecurity incident.	Enrich Disaster Recovery Plan with procedures which would apply to all computer systems, physical inventory and supplying systems (network, electricity, etc.) and also to all processes that directly or indirectly affect the organization's normal operation and environment or provide a service delivery to clients.
Maturity Level observed by UD	LEVEL 2 - MANAGED
Documents reviewed	Disaster recovery plan.docx DRP checklist

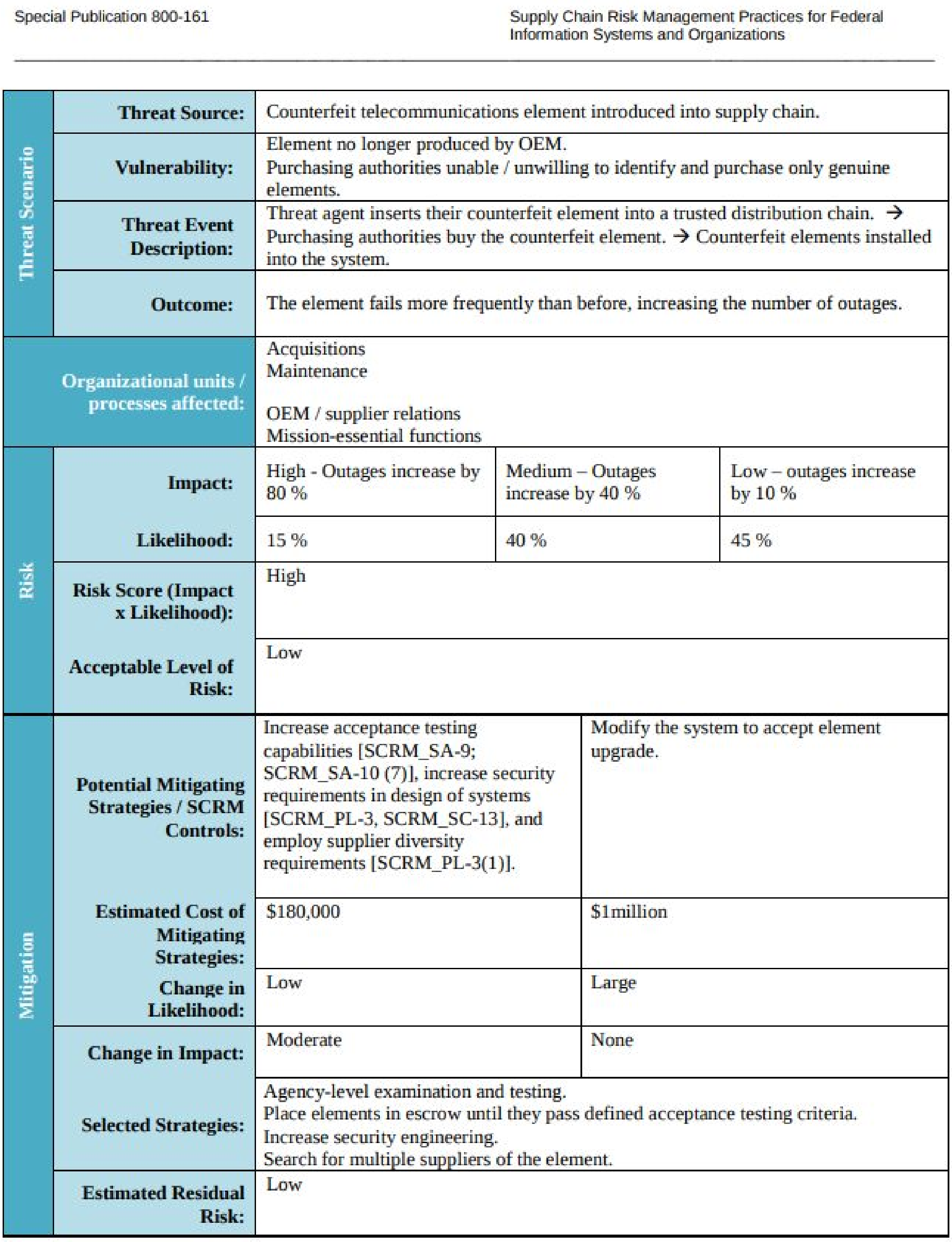
Improvements (RC.IM)

Short description	Recovery planning and processes are improved by incorporating lessons learned into future activities.
Subcategories	**RC.IM-1:** Recovery plans incorporate lessons learned **RC.IM-2:** Recovery strategies are updated
UD Observations	**UD Recommendations**
RC.IM-1: Disaster Recovery Plan plan is tested on regular basis. Lessons learned procedures was implemented after a major incident. Time for recovery procedures was significantly reduced; Last DRP testing was executed in July 2018.	Applicable lessons learned from previous incidents should also be shared with users. Improving user awareness regarding incidents should reduce the frequency of incidents, particularly those involving malicious code and violations of acceptable use policies.
RC.IM-2: Recovery strategies are updated after lessons learned phase. Formal procedures are in place. Project plan is established, roles and responsibilities are described.	The Disaster Recovery Plan should be reviewed for accuracy and completeness at least annually, as well as upon significant changes to any element of the DRP system, mission/business processes supported by the system, or resources used for recovery procedures. Elements of the plan subject to frequent changes, such as contact lists, should be reviewed and updated more frequently. Update schedules should be stated in the DRP.
Maturity Level observed by UD	LEVEL 3 - ESTABLISHED
Documents reviewed	Disaster recovery plan.docx DRP checklist

Communications (RC.CO)

Short description	Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).
Subcategories	**RC.CO-1:** Public relations are managed **RC.CO-2:** Reputation is repaired after an incident **RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams
UD Observations	**UD Recommendations**
RC.CO-1: Public relations are managed within support department and GDPR relationships; Public Relationships department manage communications related to company's products and services.	Create a procedures which will include follows things: managing media interactions, coordinating and logging all requests for interviews, handling and 'triaging' phone calls and e-mail requests, matching media requests with appropriate and available internal experts who are ready to be interviewed, screening all of the information provided to the media, ensuring personnel are familiar with public relations and privacy policies.
RC.CO-2: Reputation repair plan is developed and tested within GDPR relations. The plan describes how to handle a data breach and it's covers all essential functions related to data breaches and responsibilities are defined as well.	Implement and document crisis response strategies which will include actions to shape attributions of the crisis, change perceptions of the organization in crisis, and reduce the negative effect generated by the crisis.
RC.CO-3: There is 'How to handle data breach' process which describes communication of recovery activities via: - Public statements; - Customer notification; - Notification of Supervisory Authority. There is a Data Breach Response Team established within the process.	Write down detailed descriptions of each procedure related to recovery communication(e.g. Notify SA, Notify data subjects, Input data in data breach register, etc.) to make sure each stakeholder aware of his/her responsibilities. Consider creation of Data Breach Response Policy. For your information: https://www.sans.org/security-resources/policies/general/pdf/data-breach-response
Maturity Level observed by UD	LEVEL 3 - ESTABLISHED
Documents reviewed	How to handle a data breach.docx

Appendix B: Artifacts



Special Publication 800-161

Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Threat Scenario	Threat Source:	Counterfeit telecommunications element introduced into supply chain.		
	Vulnerability:	Element no longer produced by OEM. Purchasing authorities unable / unwilling to identify and purchase only genuine elements.		
	Threat Event Description:	Threat agent inserts their counterfeit element into a trusted distribution chain. → Purchasing authorities buy the counterfeit element. → Counterfeit elements installed into the system.		
	Outcome:	The element fails more frequently than before, increasing the number of outages.		
Organizational units / processes affected:		Acquisitions Maintenance OEM / supplier relations Mission-essential functions		
Risk	Impact:	High - Outages increase by 80 %	Medium – Outages increase by 40 %	Low – outages increase by 10 %
	Likelihood:	15 %	40 %	45 %
	Risk Score (Impact x Likelihood):	High		
	Acceptable Level of Risk:	Low		
Mitigation	Potential Mitigating Strategies / SCRM Controls:	Increase acceptance testing capabilities [SCRM_SA-9; SCRM_SA-10 (7)], increase security requirements in design of systems [SCRM_PL-3, SCRM_SC-13], and employ supplier diversity requirements [SCRM_PL-3(1)].	Modify the system to accept element upgrade.	
	Estimated Cost of Mitigating Strategies:	$180,000	$1million	
	Change in Likelihood:	Low	Large	
	Change in Impact:	Moderate	None	
	Selected Strategies:	Agency-level examination and testing. Place elements in escrow until they pass defined acceptance testing criteria. Increase security engineering. Search for multiple suppliers of the element.		
	Estimated Residual Risk:	Low		

Figure 4: Example of Threat Scenario.

From https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf

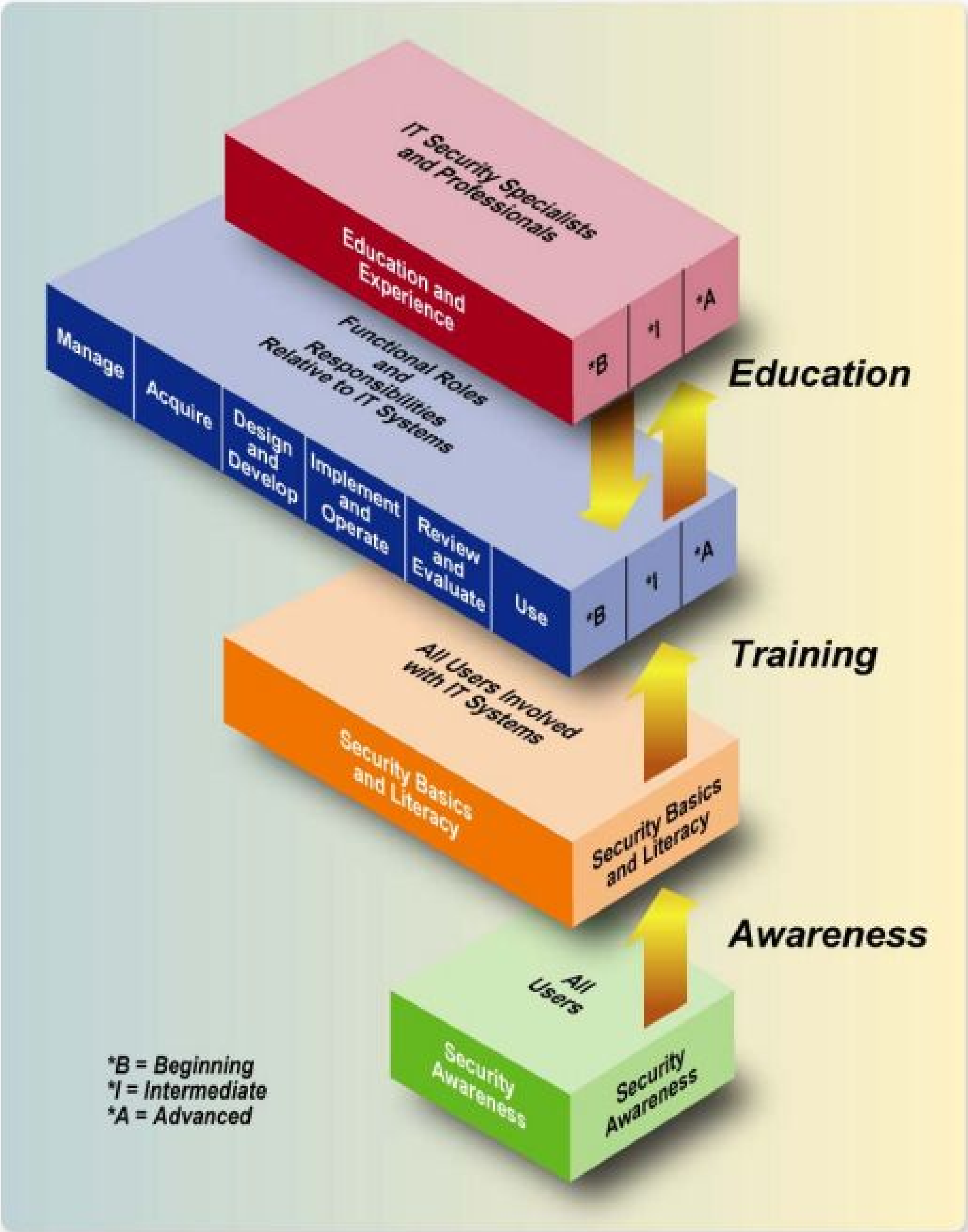


Figure 2-1: The IT Security Learning Continuum

Figure 5: The IT Security Learning Continuum
From https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf

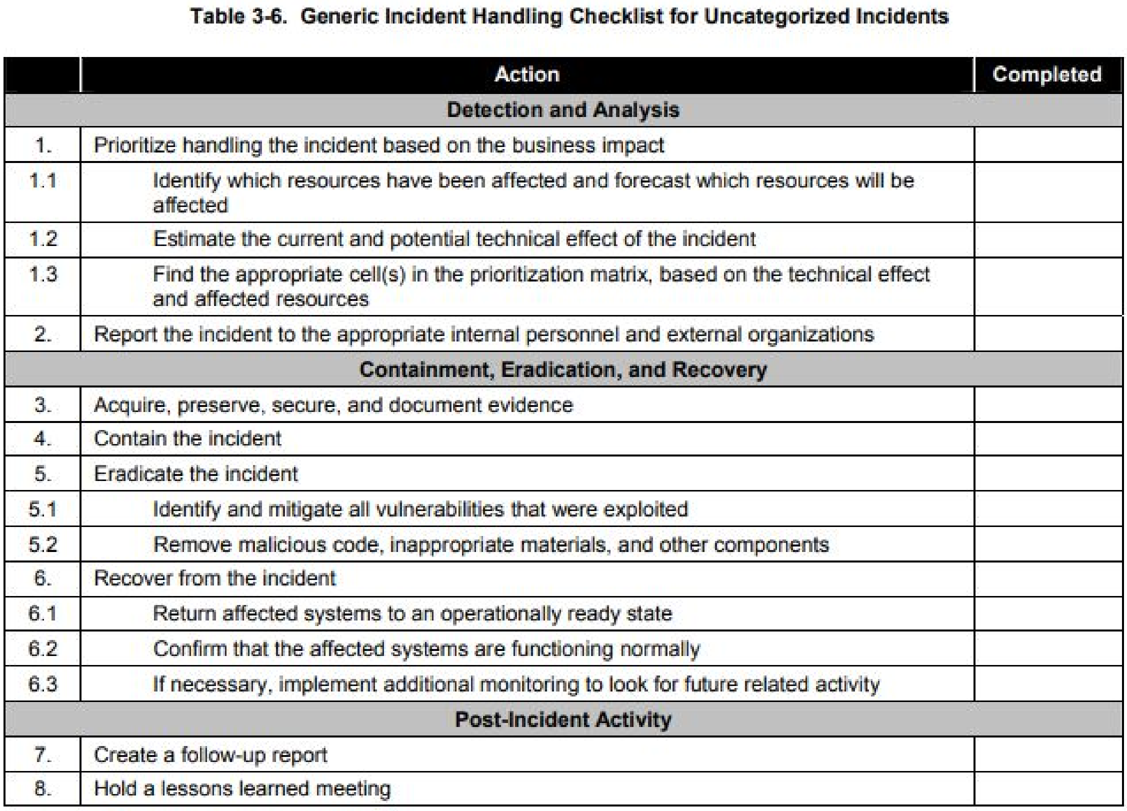


Table 3-6. Generic Incident Handling Checklist for Uncategorized Incidents

	Action	Completed
	Detection and Analysis	
1.	Prioritize handling the incident based on the business impact	
1.1	Identify which resources have been affected and forecast which resources will be affected	
1.2	Estimate the current and potential technical effect of the incident	
1.3	Find the appropriate cell(s) in the prioritization matrix, based on the technical effect and affected resources	
2.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
3.	Acquire, preserve, secure, and document evidence	
4.	Contain the incident	
5.	Eradicate the incident	
5.1	Identify and mitigate all vulnerabilities that were exploited	
5.2	Remove malicious code, inappropriate materials, and other components	
6.	Recover from the incident	
6.1	Return affected systems to an operationally ready state	
6.2	Confirm that the affected systems are functioning normally	
6.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
7.	Create a follow-up report	
8.	Hold a lessons learned meeting	

Figure 6. Generic Incident Handling Checklist for Uncategorized Incidents.
From https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-61.pdf

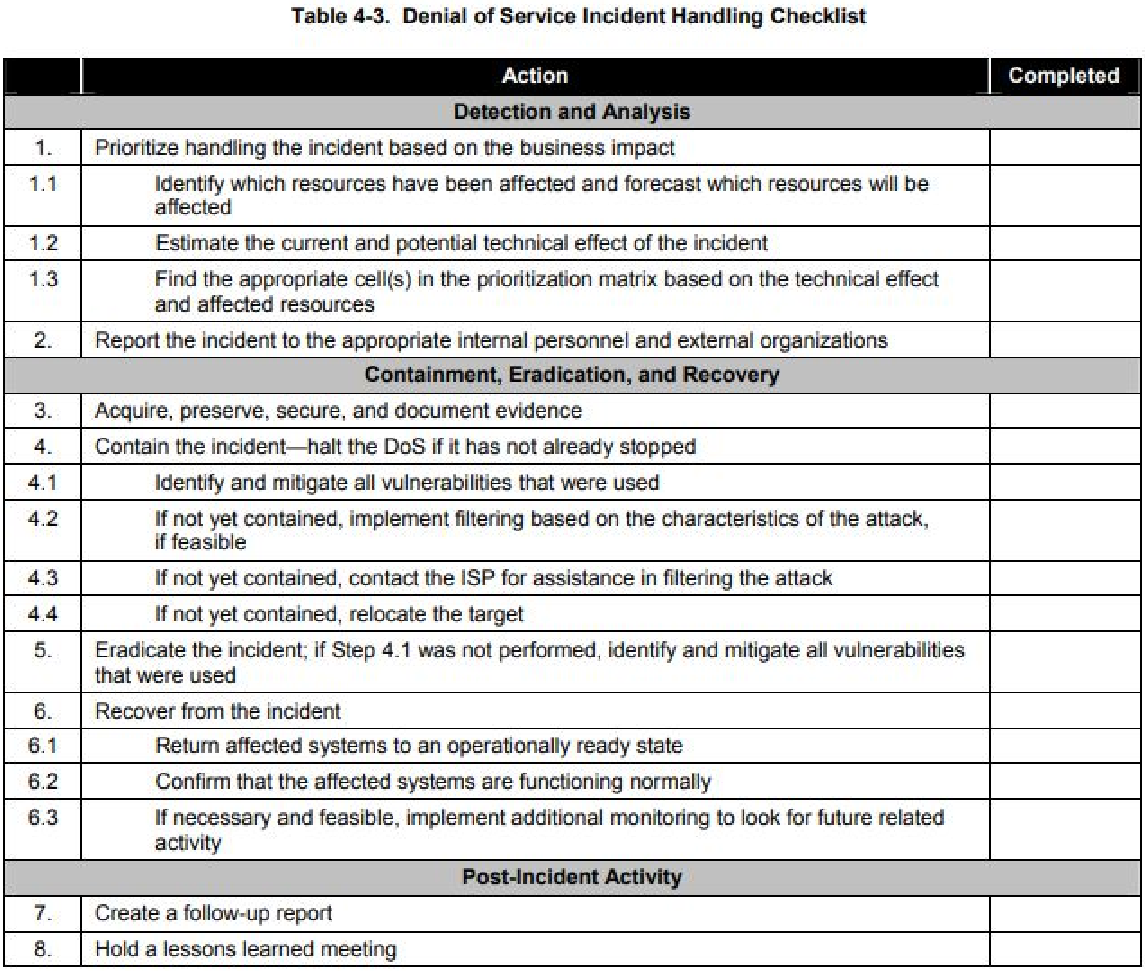


Table 4-3. Denial of Service Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Prioritize handling the incident based on the business impact	
1.1	Identify which resources have been affected and forecast which resources will be affected	
1.2	Estimate the current and potential technical effect of the incident	
1.3	Find the appropriate cell(s) in the prioritization matrix based on the technical effect and affected resources	
2.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
3.	Acquire, preserve, secure, and document evidence	
4.	Contain the incident—halt the DoS if it has not already stopped	
4.1	Identify and mitigate all vulnerabilities that were used	
4.2	If not yet contained, implement filtering based on the characteristics of the attack, if feasible	
4.3	If not yet contained, contact the ISP for assistance in filtering the attack	
4.4	If not yet contained, relocate the target	
5.	Eradicate the incident; if Step 4.1 was not performed, identify and mitigate all vulnerabilities that were used	
6.	Recover from the incident	
6.1	Return affected systems to an operationally ready state	
6.2	Confirm that the affected systems are functioning normally	
6.3	If necessary and feasible, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
7.	Create a follow-up report	
8.	Hold a lessons learned meeting	

Figure 7. Denial of Service Incident Handling Checklist
From https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-61.pdf

Summary

Within the scope of security assessment for [*Name of company]* we conducted 17 interviews with key stakeholders to value current security level within organization and review existing procedures, controls, documentation and policies. After mapping outcomes of interview and documentation analysis on NIST CSF categories we evaluated current state of Framework Profile. Radar chart was prepared to provide a graphical summary of the assessment. Roadmap was prepared as a step-by-step plan to start execute improvements on the security posture of the organization.

We recommend *[Name of company]* conducting of a Risk Assessment, creating Target Profile and to start implementing security controls one-by-one to raise them up to target level of maturity and in such way enable the organization to perform cost-effective, targeted improvements