National College of Ireland

Configuration Manual

MSc Research Project
Cyber Security

Meraz Hussain
Student ID: X21138290

School of Computing
National College of Ireland

Supervisor: Prof. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Meraz Hussain
Student ID:	X21138290
Programme:	MSc in Cyber Security **Year:** 2022-2023
Module:	Industry Internship
Lecturer:	Prof. Vikas Sahni
Submission Due Date:	05/01/2023
Project Title:	An Effective Cybersecurity Risk Assessment Framework for a Public Sector Gas Production/Distribution Company
Word Count:	1792 **Page Count:** 15

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Meraz Hussain

Date: 05/01/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Meraz Hussain
Student ID: x21138290

1 Introduction

The Configuration manual provides an overview and insights on the research conducted as part of the Academic Research Project. This study created a realistic Risk Assessment methodology to examine the key assets and cyber maturity of a critical infrastructure energy sector organization and offer changes. This handbook will provide information on the system configuration, methodology used during research, and project execution. The implementation part will walk through the process of development as well as the research findings. The internship task report is also covered in this guidebook.

2 System Configuration

The configuration of the system used during the research is as follows:

- Operating system: Windows 11
- Processor: Intel i5-11th gen
- System Compatibility: 64-bit
- Hard Disk: 512 GB SSD
- RAM: 8GB

3 Implementation

This section discusses step-by-step instruction for the execution of the proposed Risk assessment methodology for a Landfall gas pipeline site in Lougshinny, Ireland. The Lougshinny Landfall facility connects the Northern Ireland Unified Gas Transport System to the Gas Network Ireland (GNI) Pipelines.

3.1 Asset Identification and Impact Assessment

- As a first stage, the assets of the site/facility under consideration are identified, followed by the determination of possible threat scenarios that might impair the everyday function of the gas pipeline operation.
- An impact value is assigned to each asset, and those values are then used across six factors to determine the total effect.
- Based on stakeholder input, organizational standards, and best practices, it is determined how likely it is that the threat actor would exploit the vulnerability.
- The likelihood and impact are used to determine inherent risk.
- Finally, organizational countermeasures are examined for each scenario and risk is re-evaluated to determine residual risk.

Following figure shows the proposed Risk matrix to be used to assess Impact on the assets:

	Impact Factors						
	Safety	Environment	Financial	Quality	Business Continuity	Reputation & License	Impact
IMPACT	Minor Injury Loss if Visibility/Control to an Individual Site	Small Release of Gas	Equivalent to an annual economic profit impact up to Euro 100,000	Will not affect end of product/service or assurance of quality	Loss of service capacity between 1-4 working hours for one essential business process or Loss of service capacity for less than 1/2 hour for one critical business process	No Regulator Involvement	1 Trivial
	Minor Injury Requiring Outpatient treatment	Medium Release of Gas	Equivalent to an annual economic profit impact up to Euro 100,000 to Euro 500,000	Has potential to impact quality of product/service	Loss of service capacity between 1/2 to 2 days for one essential business process or Loss of service capacity for more than 1/2 hour for one critical business process	Customer Complaint	2 Minor
	Loss Time Incident	Medium to Large Release of gas	Equivalent to an annual economic profit impact up to Euro 0.5 million to Euro 3.5 million	Direclty affects quality of product/service	Loss of service capacity between 2 to 7 days for one essential business process or Loss of service capacity for more than 1 hour for one critical business process	Informal Regulator Involvement	3 Moderate
	Single Fatality orf Serious Injury	Lasting but localised damage	Equivalent to an annual economic profit impact up to Euro 3.5 million to Euro 7.5 million	Seriously affects quality of product	Loss of service capacity between 1 to 4 weeks for one essential business process or Loss of service capacity for more than 1/2 hour for one critical business process	Investigation from Regulators & Possible Sanctions	4 Major
	Multiple Facilities Loss of visibility and control to all Sites	Lasting but Widespread damage	Equivalent to an annual economic profit impact above Euro 7.5 million	Failure to meet even basic intended standards for product/service	Loss of service capacity more than 4 weeks for one essential business process or Loss of service capacity for more than 1/2 hour for one critical business process	Possible loss of license	5 Critical

(Continued to the right of above figure)

Likelihood →				
Inconceivable.May never Happen. Only in exceptional Circumstances	Possible but conisdered unlikey	Possible- Circumstances be envisaged for it to occur	Likely to happen	Will happen or highely likely to happen
1 Improbable	2 Rare	3 Unlikely	4 Possible	5 Likely
1	2	3	4	5
2	4	6	8	10
3	6	9	12	15
4	8	12	16	20
5	10	15	20	25

Figure 1 - Description of 6 Impact factors and corresponding Risk Matrix

Impact Assessment screenshots of certain assets (grouped in zones) are shown below:

				Impact												
Asset Name/ Group/ Zone	Threat Action	Vulnerabilities	Impact Description	Threat Source	S	E	F	Q	BC	R & L	Max Impact	Inherent Likelihood	Inherent Risk	Exisiting Countermeasure(s)	Residual Likelihood	Residual Risk
SCADA Comms. Zone	User accesses the configuration interface of the wired (MPLS) SCADA router and applies an incorrect configuration.	•Routers physically accessible to all on site. •Web configuration interface not restricted to OoB management port. •Default credentials in use. •Admin passwords widely-known. •DHCP enabled on network.	•Loss of comms to Grid Control SCADA •Loss of visibility/control of site from Grid Control. •Deployment of C&I technicians to site. •Recovery of configuration from backups. •Possible to run these sites "on paper"	Authorized Personnel					3		3	2	6	• Redundant SCADA routers (1 Wired, 1 GPRS/3G/4G installed on site. • TACAS used for authentication on configuration interfaces	2	6
				Authorized Personnel					3		3	3	9		2	6
				Authorized 3rd Party					3		3	2	6		2	6
				Unauthorized 3rd Party					3		3	3	9		2	6
	User accesses the configuration interface of the wireless (GPRS/3G/4G) SCADA router and applies an incorrect configuration.	•Routers physically accessible for all on site. •Web configuration interface not restricted to OoB management port.	•Loss of comms to Grid Control SCADA •Loss of visibility/control of site from Grid Control. •Deployment of C&I technicians to site. •Recovery of configuration	Authorized Personnel					3		3	2	6	•Redundant internet connections back to Grid. •Control (1 No. Wired, 1 No. GPRS/3G/4G) means multiple links to communicate back over should one	2	6
				Authorized Personnel					3		3	3	9		2	6
				Authorized 3rd Party					3		3	2	6		2	6
				Unauthorized												
	Malicious actor carries out DDOS attack on the WAN side of the SCADA routers.	No Denial of Service Attack protection mechanism used on routers	•Loss of comms to Grid Control SCADA •Loss of visibility/control of site from Grid Control. •Deployment of C & I technicians to site.	Authorized Personnel					3		3	2	6	• Physical security on site, such as the external gate mitigates this somewhat • Local SCADA on site can be used for comparison • Private connection supplied by the ISP	2	6
				Authorized Personnel					3		3	2	6		2	6
				Authorized 3rd Party					3		3	2	6		2	6
				Unauthorized 3rd Party					3		3	4	12		3	9
	Disruption to SCADA Routers mains Power supply	•System not backed up by UPS • Only ESB supply in	•Loss of comms to Grid Control SCADA •Loss of visibility/control of site from Grid Control. •Deployment of C & I technicians to site.	Miscellaneous					3		3	4	12	•UPS on sites powering critical site equipment •Backup generator onsite for automatic failover	1	3
DMZ	Malware Infection (e.g. ransomware) becomes active on the network	•Device patching is unmaintained, resulting in systems with known vulnerabilities. •Lack of network segmentation.	•Downtime due to restoring from known good, offsite backups. •Loss of confidentiality on documentation, data, network layouts	Malware	5	5	5		5	4	5	4	20	Antivirus installed on networked Windows devices	3	15
	User disrupts power to DMZ PCs	•PCs easily accessible by all on site. •No UPS Installed.	•Remote access to EWS via Jump-Box disrupted. •Loss of emissions monitoring. •IACS nodes got receiving WSUS/AV signature updates meaning they are more exposed in the event of further attack on the network.	Authorized Personnel					3		3	3	9	•UPS on sites powering these machines •Backup generator onsite for automatic failover	1	3
				Unauthorized Personnel					3		3	2	6		1	3
				Authorized 3rd Party					3		3	3	9		1	3
				Unauthorized 3rd Party					3		3	3	9		1	3
SCS Zone	Unauthorized external person (e.g., a hacker) maliciously modified alarm configurations	•No screen lock time-out on EWS PCs •No login time-out on Local SCS SCADA application, •Weak or non-existent user authentication on SCADA application	•User has access to functionality which they may not fully understand, and hence Impact system Integrity. •Loss of control with potential compromise of the safety of me process.	Unauthorized 3rd Party	5						5	3	15	•"Offline Mode" on Centum SCADA application, effectively Read-Only. •Username/Password required for Read/Write access to	3	15
	Mallcious actor carries out man-n-the-middle attack between OPC1/OPC2 and PCs and the SCS controllers, or between OPC1/OPC2 PCs and Grid Control.	•Lack of network segmentation. •Unused ports on switches not disabled •DHCP enabled on switches. •No antivirus on technician laptops. •Non-standard laptop	•Integrity of data to Grid Control SCADA may be compromised - SCADA may not accurately reflect site conditions. •Operator may take incorrect/dangerous action based on the data available e.g.	Authorized Personnel	5						5	1	5	•Multiple levels of physical security (outer gate, main building entry) to get through •Antivirus running on machine •Vendor manage these machines regarding	2	10
				Unauthorized Personnel	5						5	2	10		2	10
				Authorized 3rd Party	5						5	1	5		4	20
				Unauthorized 3rd Party	5						5	4	20		3	15

Figure 2 - Proposed Impact Assessment Sample Template with few use cases

After the impact assessment, a Network Diagram is constructed for the site exhibiting essential assets with similar residual risk ratings in Zones. The network diagram from the impact evaluation is below:

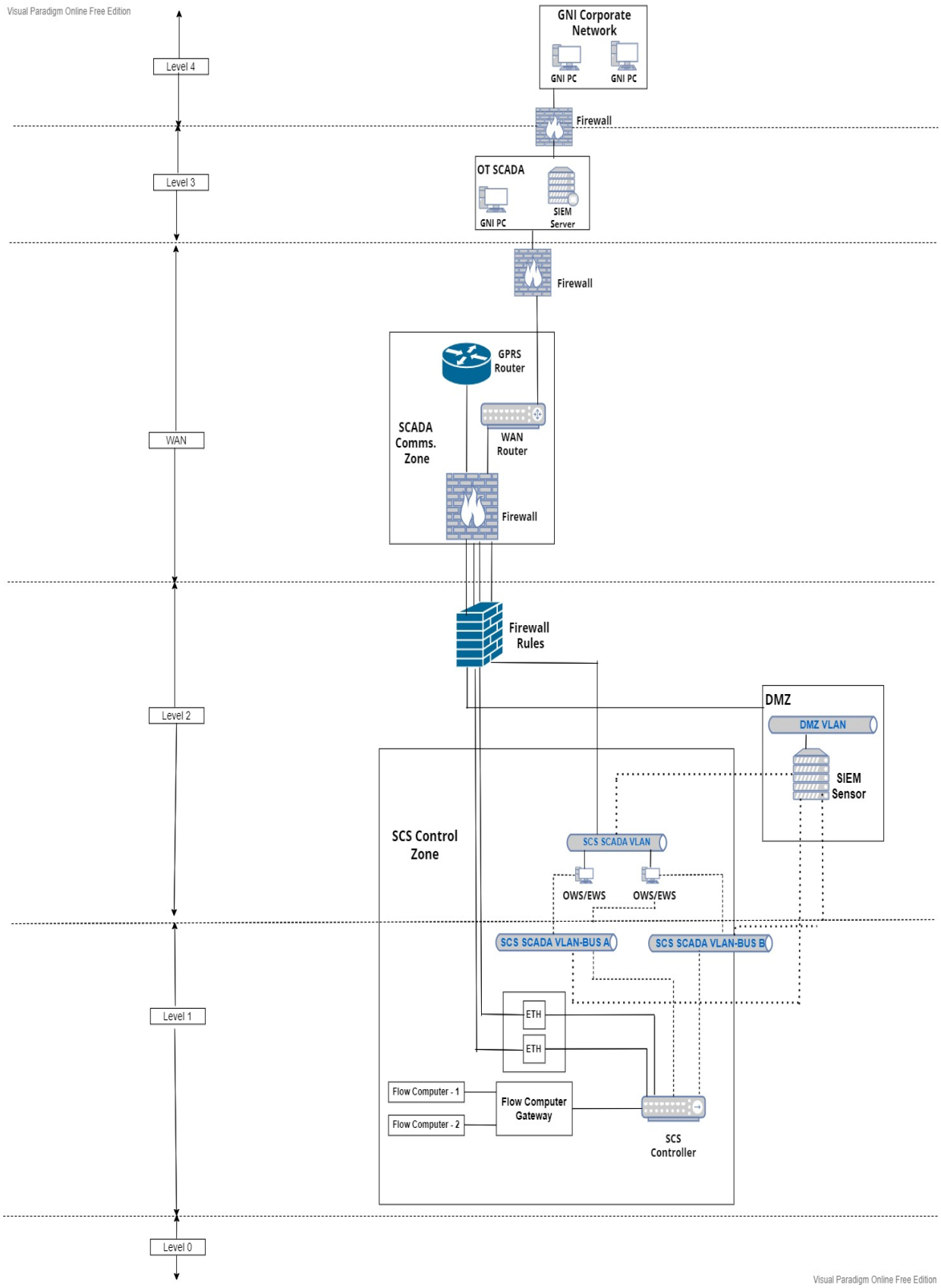

Figure 3 - Lougshinny Site High Level Network Diagram based on Impact Assessment

3.2 Detailed Risk Assessment using NIST CSF

Each CSF category is given a score of 0, 0.5, or 1 depending on how well it aligns with the suggested goals outlined in Figure 4. This information is then used to calculate a maturity score for each of the 5 CSF functions. This model evaluates 108 CSF controls/subcategories for a natural gas production facility based on the following four objectives:

a) Operational objective of the controls and cybersecurity processes
b) Design objective of the controls and cybersecurity processes
c) Implementation objective of controls and cybersecurity processes
d) Review frequency of the controls

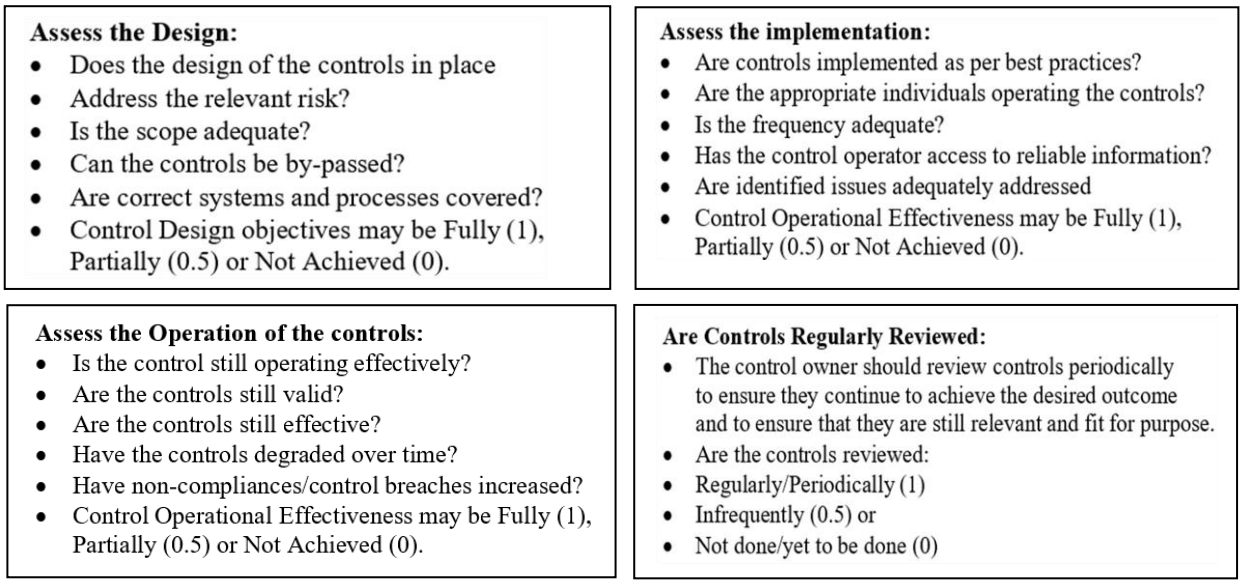

Figure 4 – Risk Assessment Proposed Objectives

Below Figures shows some of the control testing that was done on few controls in the Identify function, since it is not feasible to include screenshots of all the controls of 5 functions:

Category	Subcategory	Controls in place	Control Owner	Design Assessment	Implementation Assessment	Operational Assessment	Control Review	Gaps in the controls
Asset Management (ID.AM): 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 business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	BCP Framework Refresh -Consolidation of Group, EBS and GNI materials. Review of scenarios, to be prioritised in order of business impact/criticality, development plans to be put in place for high priority response plans (Cyber, Security of Supply, Single Source Supplier etc.) 2022 Business Continuity Exercise Programme - Co-ordination of our annual business continuity exercise plan in line with our business continuity framework guidelines. (2022 exercise plan available upon request).	Security & Operations Technology Manager	Partially Achieved	Partially Achieved	Partially Achieved	Yet To Be Done	An informal check of the Core Asset register is performed quarterly but this is not under any governed control No formal Control Monitoring - Policies and Procedures to be developed to formally govern the management, maintenance and monitoring of controls — to ensure inventory controls operate as intended. GNI must install an appliance in the Enterprise and O.T. Core to discover/report on equipment installed on the site network The Operational impact of loss of availability of systems should be categorised. Details of all high impact systems are captured Automated discovery/detection tools should be used to collect inventory data.
	ID.AM-2: Software platforms and applications within the organization are inventoried	For Core Assets there is an up to date software inventory in place through the application landsweeper. A copy of the latest software inventory can be provided upon request. It lists the following : Asset Name, Software, Version, Publisher, OS, Domain, Install Date OT Core utilize WSUS (Windows Update Pogram), Ansible (Red Hat), Oracle Enterprise Manager and VMware vCentre discovery components for managing hardware and software implementations. Cyber security site surveys have been completed and assesment on three sites have taken place. The detailed design is ongoing with the plan to	Security & Operations Technology Manager	Partially Achieved	Partially Achieved	Partially Achieved	Yet To Be Done	An up to date record of Software inventory which underpins each Critical Activity should be maintained The inventory should capture details such as: Business Owner, L'CenCes, Warranty, EoL For OT/ICS assets the inventory captures information such as: Model, Type, Firmware revision The inventory captures details of software maintained by a 3rd party Software licences are managed. Hardware and Software inventories are integrated.

Figure 5 - Risk Assessment for few Identify subcategories

Category	Subcategory	Controls in place	Control Owner	Design Assessment	Implementation Assessment	Operational Assessment	Control Review	Gaps in the controls
Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	RBAC controls based on least privilege are documented and implemented for determining access to Core systems. All access requests go through the Enterprise ServiceNow portal with appropriate authorisations. User access reviews carried out every quarter. In addition to the OT UAR process the OT team have implemented an automated process which ensure user accounts are disabled after 30 days of inactivity and retired after 90 days. They recieve a weekly summary of users who will be disabled and retired if left inactive, and a summary of 3rd party admin accounts who are currently enabled. Contractors access is timebound for the specific duration of the support task. There is a password policy and standard document in place which outlines length, complexity, change	Infrastructure Security Manager	Partially Achieved	Partially Achieved	Partially Achieved	Regular (0-12 Months)	Indicators of Good Practice Multifactor Authentication is used to control access to network devices (e.g., servers, workstations, mobile devices, firewalls) MFA is used to control access to Privileged Access and Administration Accounts Only authorised and individually authenticated users can physically access and logically connect to critical networks or information systems. One-time passwords are issued for temporary access to the network.
	PR.AC-2: Physical access to assets is managed and protected	Security Services Provided 1. Manned Security Services - Security System Maintenance Contracts - Remote Monitoring - Monthly Meetings and KPIs 2.Remote Monitoring and Incident Management -Remote arming/disarming Procedures and reporting - Incident	Facilities Manager	Fully Achieved	Fully Achieved	Fully Achieved	Regular (0-12 Months)	N/A
	PR.AC-3: Remote access is managed	JML process for remote access as in PR.AC-I with UARs performed regularly. All Remote access over Citrix Netscaler using (SecurelD) soft token 2FA. Depending on the criticality of the asset and application a 3rd party vendor may be required to attend on site. If required on site they will be supervised and if done remotely their	Infrastructure Security Manager	Partially Achieved	Partially Achieved	Partially Achieved	Yet To Be Done	There is no list of third-party authorised list but named users who have previous exposure to the GNI environment. No control or metric in place Indicators of Good Practice Remote users' Policies and procedures ensure: •Remote users

Figure 6 - Risk Assessment for few Protect subcategories

Category	Subcategory	Controls in place	Control Owner	Design Assessment	Implementation Assessment	Operational Assessment	Control Review	Gaps in the controls
Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	There is a baseline of expected dataflows established and is implemented through network routing rules and technicalcontrols such as f irewalls and IDS IPS. These logs are now sent to the SOC/SIEM and the threat cases will determine what events are triggered. Additional compliance will be acheieved through the SIEM OT project.	IT Strategy and Performance Delivery Manager	Partially Achieved	Partially Achieved	Partially Achieved	Yet To Be Done	Must implement a network management policy and agree a timeframe to review the network management policy. Once created this will outline how often we review our network/data flows diagrams.A metric for this control needs to be created.
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	implemented through network routing rules and technical controls such as firewalls and IDS / IPS. These logs are now sent to the SOC/SIEM and the threat cases will determine what events are triggered. Additional compliance will be acheieved	Security and Operations Technology Manager	Partially Achieved	Partially Achieved	Partially Achieved	Regular (0-12 Months)	Controls need to be implented to measure and report on monthly metrics
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	SIEM Correlation Searches will alert against a base event severity which is pre determined per Correlation Search. The event severity is combined with the priority of the host and/or user to create the Alert Urgency, to which the Managed Service SLA applies. The list of	Security and Operations Technology	Partially Achieved	Partially Achieved	Partially Achieved	Regular (0-12 Months)	Validation of event data needs to be carried out regularly as opposed to on an adhoc basis. Real time updates should be considered due to being a critical infrastructure. Indicators of Good Practice All new systems are considered

Figure 7 - Risk Assessment for few Detect subcategories

Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	The Information Security Incident Policy describes the roles and responsibilities of the SIRT team which must be formed for all Sev 1 and 2 incidents. Roles which make up the SIRT include: •SIRT Coordinator - ISDP Representative •Information Security - Information Security Lead •Security & Investigations - Security & Operations Technology Manager •Data Protection - DO & FOI Officer	Organisation Change Lead	Partially Achieved	Partially Achieved	Partially Achieved	Yet To Be Done	Roles and responsibilities should be defined in the incident response plan, including the role of external contractors and incident response teams. Relevant personnel should know their roles and responsibilities and should be trained on the Incident Response plans and take part in relevant response plan tests. Training should covers employee roles and responsibilities in the event of an incident. Third party/supplier/contractors roles and responsibilities should be called out in the incident response plan
	RS.CO-2: Events are reported consistent with established criteria	While the Ervia Information Security Incident Policy covers the GNI Group and its operating companies (Gas Networks Ireland and Aurora) and any of its subsidiaries in any geographic region. The policy is cognizant of the legal and regulatory requirements for notifying relevant parties in the event of an incident. Policy statement regarding NIS D and GDPR. Where it is necessary to notify a third party of an Information Security incident (including reporting obligations under NIS and GDPR), this will be managed exclusively by the Security Incident Response Team (SIRT) and the	Head of Legal Affairs	Fully Achieved	Fully Achieved	Partially Achieved	Yet To Be Done	Reporting structure and communication channels should be clearly defined in the incident response plan.

Figure 8 - Risk Assessment for few Respond subcategories

Category	Subcategory	Controls in place	Control Owner	Design Assessment	Implementation Assessment	Operational Assessment	Control Review	Gaps in the controls
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	RC.RP-1: Recovery plan is executed during or after an event	There is a lessons learned exercise following each incident and the recovery plans are revisited and updated as required, however the documentation of the recovery plans is not mature so there is no clear tracking of the lessons learned in the documentation.	Infrastructure Management Manager	Partially Achieved	Partially Achieved	Partially Achieved	Yet To Be Done	Metric / Control should be created to demonstrate documentation is reviewed and testing takes places annually. Better documentation to demonstrate the following needs to be reviewed & improved or created: •Business continuity plan, •Incident response plan, •Disaster recovery plan, •Cybersecurity incident plan, •Run-books Plans contain steps and procedures for common threats, triggers for activation, RPOs and RTOs.
Improvements (RC.IM): Recovery planning and processes are improved by incorporating	RC.IM-1: Recovery plans incorporate lessons learned	During an incident there are a number of roles within the SIRT with responsibility for maintaining communications across a range of stakeholders: Stakeholder Representative - Each	Infrastructure Management Manager	Partially Achieved	Partially Achieved	Partially Achieved	Yet To Be Done	Plans and procedures need to be reviewed, updated and approved on a regular basis or as changes are made to systems and controls. After cybersecurity events or tests, plans and procedures are reviewed and updated. This will ensure they are adhering to the indicators of good practice.

Figure 9 - Risk Assessment for few Recover subcategories

3.3 Evaluation of Company's Current vs Target Cyber Maturity Level/Tier

Following the scoring system developed and discussed in section 3.2, controls in each of the functions are assigned scores and average for each category is calculated. An example to demonstrate few Identify category is show below:

Category	Subcategory	Design Assessment	Implementation Assessment	Operational Assessment	Control Review	Score	Average
Identify							
Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	0.5	0.5	0.5	0	1.5	1.67
	ID.AM-2: Software platforms and applications within the organization are inventoried	0.5	0.5	0.5	0	1.5	
	ID.AM-3: Organizational communication and data flows are mapped	0.5	0.5	0.5	0	1.5	
	ID.AM-4: External information systems are catalogued	0.5	0.5	0.5	0	1.5	
	ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	0.5	0.5	0.5	0	1.5	
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	0.5	0.5	0.5	1	2.5	
Business Environment (ID.BE)	ID.BE-1: The organization's role in the supply chain is identified and comamunicated	0.5	0.5	0.5	1	2.5	
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	0.5	0.5	0.5	0	1.5	
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	0.5	0.5	0.5	0	1.5	2.5
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	0.5	0.5	0.5	0	1.5	
	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)	0.5	0.5	0.5	0	1.5	
Governance (ID.GV)	ID.GV-1: Organizational information security policy is established	1	1	1	1	4	4
	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	0.5	0.5	0.5	1	2.5	
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	1	1	0.5	1	3.5	
	ID.GV-4: Governance and risk management processes address cybersecurity risks	1	1	0.5	1	3.5	
Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented	0.5	0.5	0.5	0.5	2	
	ID.RA-2: Cyber threat intelligence and vulnerability information is received from information sharing	1	1	1	1	4	

Figure 10 – Calculation of few Identify Category individual and average scores

Similarly, all the other functions are assessed and scores for each category is calculated as captured below:

		Target Score (Q4-2022)	GNI Current Score (Q4-2022)
	Overall	**3.00**	**2.33**
Identify	Asset Management (ID.AM)	3.00	1.67
	Business Environment (ID.BE)	3.00	2.50
	Governance (ID.GV)	3.00	4.00
	Risk Assessment (ID.RA)	3.00	2.00
	Risk Management Strategy (ID.RM)	3.00	4.00
	Supply Chain Risk Management (ID.SC)	3.00	2.50
Protect	Identity Management and Access Control (PR.AC)	3.00	2.29
	Awareness and Training (PR.AT)	3.00	3.20
	Data Security (PR.DS)	3.00	1.50
	Information Protection Processes and Procedures (PR.IP)	3.00	2.63
	Maintenance (PR.MA)	3.00	2.25
	Protective Technology (PR.PT)	3.00	2.20
Detect	Anomalies and Events (DE.AE)	3.00	1.90
	Security Continuous Monitoring (DE.CM)	3.00	2.63
	Detection Processes (DE.DP)	3.00	2.80
Respond	Response Planning (RS.RP)	3.00	1.50
	Communications (RS.CO)	3.00	2.60
	Analysis (RS.AN)	3.00	2.30
	Mitigation (RS.MI)	3.00	2.17
	Improvements (RS.IM)	3.00	1.50
Recover	Recovery Planning (RC.RP)	3.00	1.50
	Improvements (RC.IM)	3.00	1.50
	Communications (RC.CO)	3.00	2.50

Figure 11 – GNI's Current vs Target NIST CSF Function's scores

The following spider diagrams illustrate the maturity levels for each function:

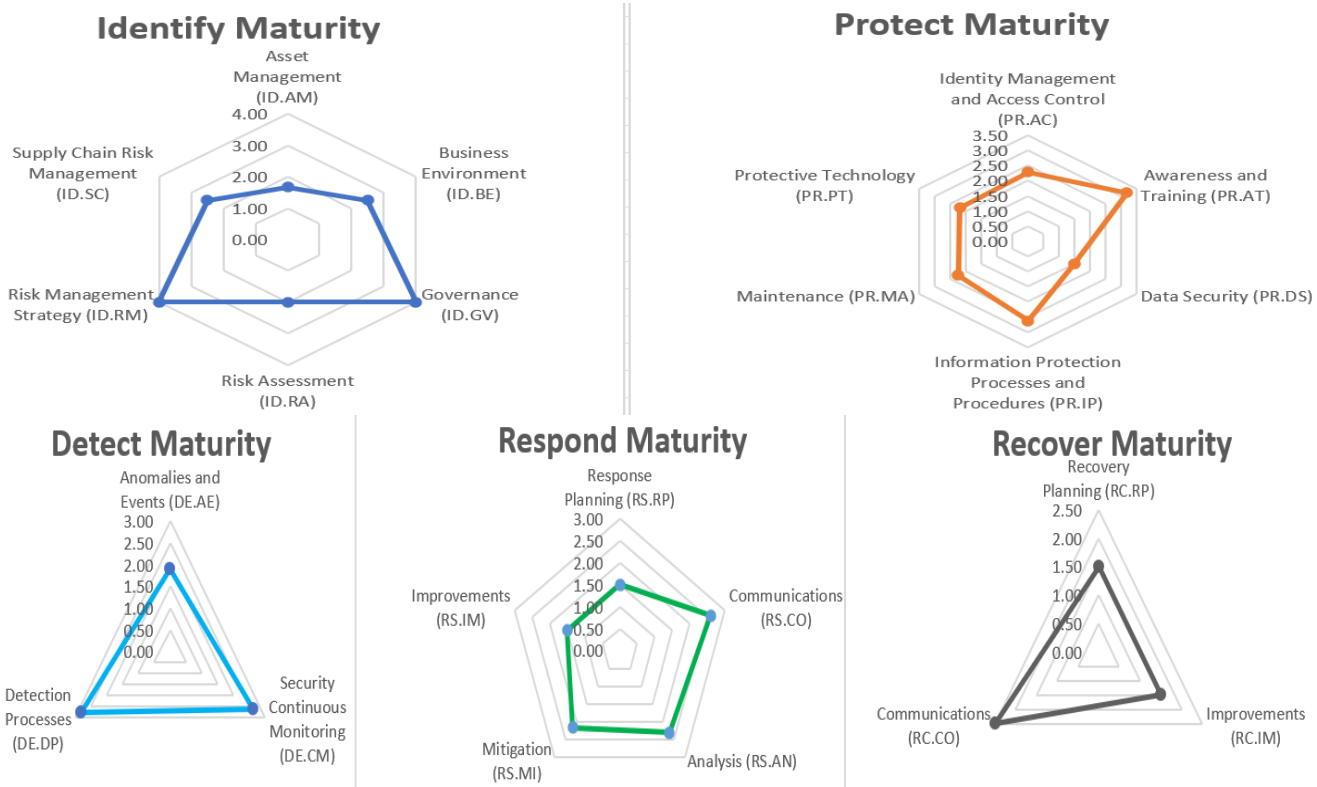

Figure 12 – GNI's Individual Functions NIST CSF Current Maturity vs Target scores

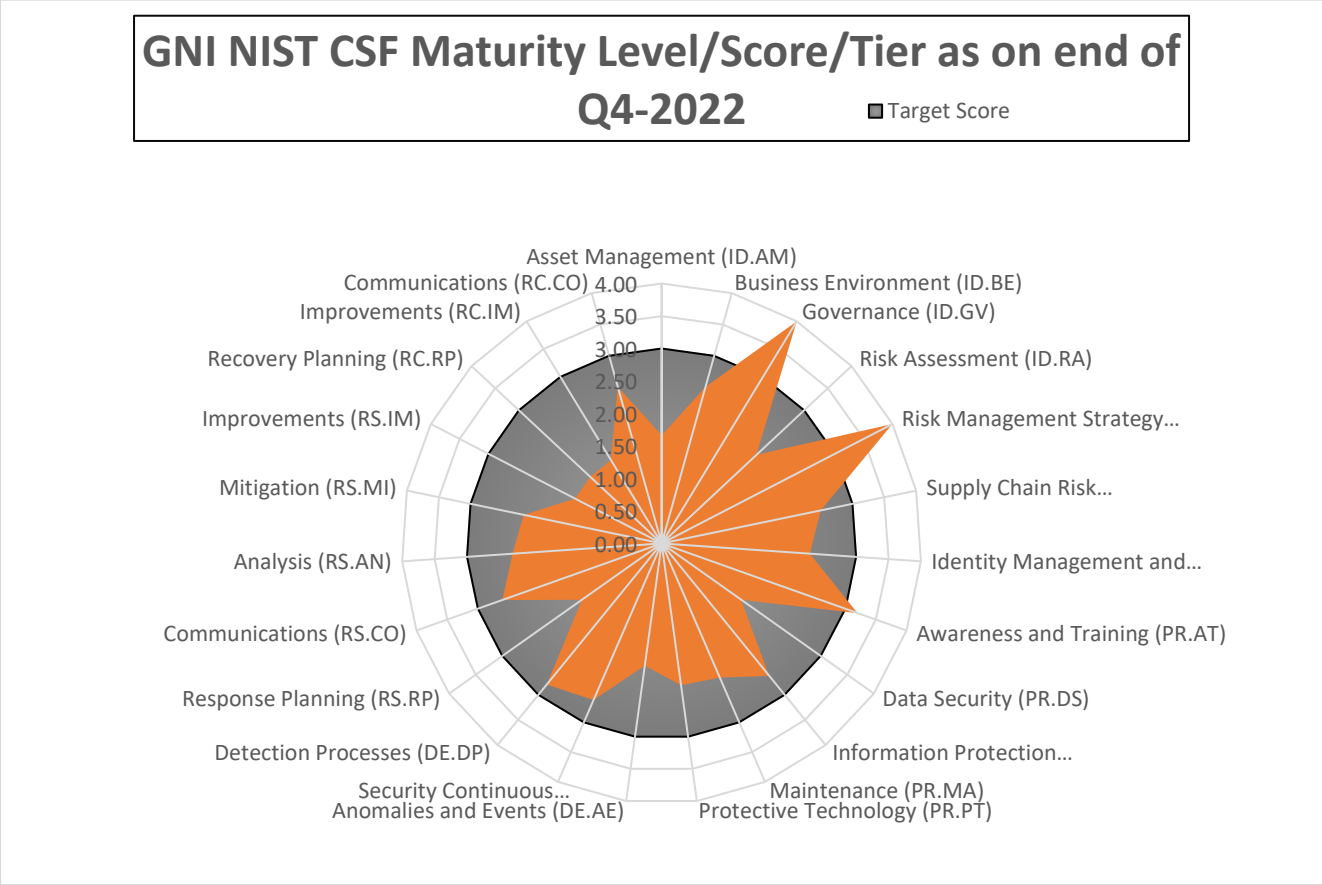

Figure 13 – GNI's Overall NIST CSF Current Maturity vs Target scores

3.4 Preparing Corrective Action Plans to meet Target Cyber Maturity level/Tier

Final phase is to develop corrective action plan to fix the gaps found in the control testing of NIST controls. The remediation plan uses the International Electrotechnical Commission (IEC) 62443-2-1 and IEC 62443-3-3 standards as guidance for secure control design and security criteria for each of the identified gaps.

Corrective Action Plan					
Identify					
Category	**Controls in Place/Current Profile**	**Gaps/ Residual Risk Identified**	**Risk Rating (H/M/L)**	**Risk Owner Assigned**	**Remediation Activity/ Project/Timeline**
Asset Management (ID.AM)					
ID.AM-1: Physical devices and systems within the organization are inventoried	BCP Framework Refresh -Consolidation of Group, EBS and GNI materials. Review of scenarios, to be prioritised in order of business impact/criticality, development plans to be put in place for high priority response plans (Cyber, Security of Supply, Single Source Supplier etc.) 2022 Business Continuity Exercise Programme - Co-ordination of our annual business continuity exercise plan in line with our business continuity framework guidelines. (2022 exercise plan available upon request).	An informal check of the Core Asset register is performed quarterly but this is not under any governed control No formal Control Monitoring - Policies and Procedures to be developed to formally govern the management, maintenance and monitoring of controls — to ensure inventory controls operate as intended. GNI must install an appliance in the Enterprise and O.T. Core to discover/report on equipment installed on the site network The Operational impact of loss of availability of systems should be categorised. Details of all high impact systems are captured Automated discovery/detection tools should be used to collect inventory data.	Medium		
ID.AM-2: Software platforms and applications within the organization are inventoried	For Core Assets there is an up to date software inventory in place through the application landsweeper. A copy of the latest software inventory can be provided upon request. It lists the following : Asset Name, Software, Version, Publisher, OS, Domain, Install Date OT Core utilize WSUS (Windows Update Pogram), Ansible (Red Hat), Oracle Enterprise Manager and VMware vCentre discovery components for managing hardware and software implementations. Cyber security site surveys have been completed and assesment on three sites have taken place. The detailed design is ongoing with the plan to implement IEC 62443. The recommendation to install an appliance in the O.T. Core to discover/report on equipment installed on the site network e.g. Claroty, or similar will be addressed through the GNI OT	An up to date record of Software inventory which underpins each Critical Activity should be maintained The inventory should capture details such as: Business Owner, L'CenCes, Warranty, EoL For OT/ICS assets the inventory captures information such as: Model, Type, Firmware revision The inventory captures details of software maintained by a 3rd party Software licences are managed. Hardware and Software inventories are integrated.	High		

ID.AM-2: Software platforms and applications within the organization are inventoried	For Core Assets there is an up to date software inventory in place through the application landsweeper. A copy of the latest software inventory can be provided upon request. It lists the following : Asset Name, Software, Version, Publisher, OS, Domain, Install Date OT Core utilize WSUS (Windows Update Pogram), Ansible (Red Hat), Oracle Enterprise Manager and VMware vCentre discovery components for managing hardware and software implementations. Cyber security site surveys have been completed and assesment on three sites have taken place. The detailed design is ongoing with the plan to implement IEC 62443. The recommendation to install an appliance in the O.T. Core to discover/report on equipment installed on the site network e.g. Claroty, or similar will be addressed through the GNI OT Security program.	An up to date record of Software inventory which underpins each Critical Activity should be maintained The inventory should capture details such as: Business Owner, L'CenCes, Warranty, EoL For OT/ICS assets the inventory captures information such as: Model, Type, Firmware revision The inventory captures details of software maintained by a 3rd party Software licences are managed. Hardware and Software inventories are integrated.	High
ID.AM-3: Organizational communication and data flows are mapped	For Core Assets, detailed connections & data flows are available for the GTMS & Scada application. Mapping of the remaining Core Asset estate is currently ongoing as part of the Network Virtualization & Security Software NSX project. Cisco ACI will handle "MacroSegmentation" — grouping machines into zones with common firewall rules. VMware NSX will then perform "Micro-Segmentation" over this delivering "Zero-Trust" between assets. Cyber security site surveys have been completed and assesment on three sites have taken place. The detailed design is ongoing with the plan to implement IEC 62443.The following documents can be provided by the OT Core team: Networking High-level Architecture "Mid-Level Design" Visio/PDFs network drawings — includes external links to corporate, internet, WAN - Spreadsheets for IP allocations, port allocations, rack layouts, cable schedule, and firewall rules. Additional detailed network drawings (Firewalls, Netscalers, Vodafone, etc.) Supporting Services - GoAnywhere application manages file based data exchanges between systems on OT networks "GoAnywhere Reference Architecture.vsdx" contains System block	Some data flow information is avaialble between connected systems. However, complete data flow mapping is not done. System interconnections need to be documented; this includes 3rd party and remote access. This may include Organisation communication diagrams.	Medium

Figure 14 – Corrective Action Plan Screenshot

Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you andwhat you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Meraz Hussain Student number: x21138290

Company: PFH Technologies Month Commencing: October-2022

- Meeting with of Gas Networks Ireland (GNI) Infosec and compliance teams to discuss the scope sites location and relevant functions.
- Gaining knowledge about ICS and OT cybersecurity and how is GNI keeping its sites safe from cyber-attacks.
- Brainstorming session with industry supervisor on various thesis/project topic by understanding the scope at which the work could be done.
- Understanding daily operation(s) as well as limitations of the site which was picked for the topic
- Selecting the topic and creating research question whilst getting agreement from Industry Supervisor.

Employer comments

Meraz is not only prompt, efficient, and has brought his past cybersecurity experience very well in the context of his work in overseeing our NIS directive compliance efforts but he has also followed the advice offered and is ready to start on his dissertation. The topic he selected would assist us in obtaining a framework that we want to employ to perform a Self-Assessment of our cyber security measures for various sites.

Student Signature: Meraz Hussain Date: 30/10/2022

Industry Supervisor Signature: John Ballentine Date: 31/10/2022

Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you andwhat you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Meraz Hussain Student number: x21138290

Company: PFH Technologies Month Commencing: November-2022

- Discussion with supervisor on the approach for the creation of Impact factors for assessing site's (under consideration) IACS cybersecurity maturity.
- Development of the six impact factors that could impact Assets on the site and establishing baseline for the scores to be assigned to each asset grouped in zone.
- Creation of the NIST CSF questionnaire based on the four-control objective mutually agreed with the supervisor.
- Agreed on approach to reach out to Control Owner(s) of the controls to be assessed.
- Carried out the Risk Assessment for the site by requesting control and policy artefacts as well as performing site visit.
- Documented response received and observed for 70 NIST CSF controls as requested during onsite visit and request for information.

Employer comments

Meraz has been able to take the lead of his dissertation and have proactively reached me for help at various checkpoints. He is always curious about different working of the ICS infrastructure at the Lougshinny site and have gained good amount of knowledge of the controls implemented. His way of coordinating with stakeholders is efficient and proactive.

Student Signature: Meraz Hussain Date: 28/11/2022

Industry Supervisor Signature: John Ballentine Date: 30/11/2022

Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you andwhat you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Meraz Hussain Student number: x21138290

Company: PFH Technologies Month Commencing: December-2022

- Obtained the response for remaining 38 controls and documented them in the questionnaire.
- Assessed and analyzed the response and artefacts received for the controls and evaluated the scores in terms of their compliance with developed controls objectives.
- Evaluated the maturity level for each of the 4 NIST CSF functions and compared those with GNI's target maturity level (3).
- Created Corrective action plan for the gaps in the controls identified and assessed.
- Advised various defense in depth options to GNI board members for some of the controls which are not implemented or lacked sufficient security at the assessed site.
- Report writing

Employer comments

As the internship draws to a close, the last month's work has been outstanding. Meraz has even led the way in delivering the pilot NIST Metrics project in its whole. We think the risk assessment questionnaire is solid and will use it to conduct in-house cyber security audits. We are really grateful to Meraz for all of his hard work and invaluable contributions throughout his internship. He's been an absolute joy to work with. Wish him all the best for his future endeavors.

Student Signature: Meraz Hussain Date: 19/12/2022

Industry Supervisor Signature: John Ballentine Date: 23/12/2022