THE UTILISATION OF NIST AS A CYBERSECURITY FRAMEWORK IN HIGHER EDUCATION INSTITUTES DURING COVID-19

NIST Cybersecurity Framework Audit & Cyber Readiness Survey

by

Thomas Hughes

C00231519

APRIL 29, 2022

Supervisor: Christopher Staff

Abstract

This document includes a NIST CSF Audit performed on a sample HEI and includes a Cybersecurity Readiness Survey aimed at multiple different Irish Higher Education Institutions. The aim of these two is to both understand how a sample HEI in Ireland is when measured against the NIST Cybersecurity Framework, conclude results about that HEI, and gain a focused scope of how competing HEIs may be in comparison to each other.

Table of Contents

Introduction

This document is the follow up to my previous document, the NIST CSF Audit, and the Cybersecurity Readiness Survey. The first document's aim was a process to perform a NIST-certified audit to assess the varying security elements of the anonymous Higher Education Institute. The second part of the project is the Cybersecurity Readiness Survey, a survey designed for IT personnel operating in HEIs around Ireland to assess a basic understanding of each HEIs cybersecurity. The questions are based on the NIST framework, and not only aim to give a general assessment on an HEIs cyber preparedness, but also allows the HEIs to be compared to each other.

Document Brief

Following the results of this audit, this document will provide recommendations in each category based on the advice given by NIST and other professional guides (listed in references) and my personal advice as an IT security student. The NIST audit is defined by functions (Identify, Protect, Detect, Respond, Recover) and its subcategories that are identified by abbreviated versions of each function, followed by the subcategory number e.g. RS.MI-5, ID.BE-2. This document will run through each function and category, defining the company's status of achieved or not, and comment on how the company did or didn't achieve this, followed by a final recommendation to move towards this achievement.

Privacy Disclaimer for Audit

The HEI, both as an entity and its members of staff that were assessed in this audit will be referred to as "named organisation" or "named HEI" to exercise this anonymity. Please contact my project supervisor staff.chris@itcarlow.ie or myself c00231519@itcarlow.ie to discuss any concerns with the identity of this HEI, and a reference can be given based on their discretion.

Privacy Disclaimer for Survey

Inclusion of the disclaimer meant users would be ensured of their protection of privacy and that the data they were providing is secure and anonymized. The disclaimer reads:

DISCLAIMER: The following survey is for research purposes ONLY. All answers will be completely anonymized. Any results of the survey will be available by request. The following questions are designed to assess HEI's cybersecurity readiness based on the NIST framework.

For any concerns or questions, please contact my supervisor chris.staff@itcarlow.ie or myself C00231519@itcarlow.ie

The disclaimer is essential in this type of research, particularly the handling of sensitive data. The data received from the survey would be deemed somewhat private, as they ask for certain providers, an estimate of services and entities found in the organisation, and overall they are being asked about how secure they are. From a legal point, this allows this survey to be within GDPR regulations, which all HEIs (hopefully) will require. It also allows those who aided in answering the audit to feel ensured about the integrity of their identities.

NIST CSF Audit

Audit Layout

The NIST security audit is a review/examination to quantify the success of the recorded entities that belong to the organization, particularly the organizations actors (e.g. devices, software, services, users, employees, board of management) and the policies that outline operational control and enforce how they them. NIST has a few different audits based on each framework, all of which roughly follow the 5 main categories (Identify, Protect, Detect, Respond, Recover) but for the sake of research in this context, we will use the NIST CSF audit.

The NIST CSF audit stems directly from the 5 main categories of the NIST framework; Identify, Detect, Protect, Respond, Recover, and their respective subcategories. The aim of using NIST was that its recognition as a reliable framework to develop an organization dynamically and would give a standard to measure how successful Higher Education Institutes were performing.

This NIST CSF was performed on an HEI whom I met the acting IT Operations manager for. We sat and discussed each segment of the NIST CSF, which I then provided the recommendations for.

Audit Process

Following the results of the audit, here are the observations made during this process. These are noted in the left column, where the recommendations to improve on the subcategory are on the right.

Identify

Asset Management

Category	Subcategory	In Compliance
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 organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**Yes**
	ID.AM-2: Software platforms and applications within the organization are inventoried	**No**
	ID.AM-3: Organizational communication and data flows are mapped	**No**
	ID.AM-4: External information systems are catalogued	**Yes**
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**Yes**
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**No**

Results	Suggestions & Recommendations
ID.AM-1. A manual asset management for inventory is documented, updated, and enforced for internal/ external machines & devices. No use of automated tools, requires word-of-mouth to notify updates of user changes	Asset management is compliant. Automated tools for ease of use would be recommended, such as Auvik (or similar), used for asset discovery on a network, or use of integrated asset checker existing in services. As a smaller college, can be achieved without.

ID.AM-2. Some software platforms and apps are inventoried, not all. Aware of this issue, currently building manual inventory for this. Some verification is needed for new software downloads.	Utilise a reliable IT software asset manager such as SolarWinds Service Desk or LanSweeper to help identify, record and label pre-existing software. Awareness and information given by users responsible for recording software are well-informed, use of APIs to share software news and updates could be used. Testing of new and existing software to be used on safe virtual machine environment.
ID.AM-3. Some ports managed & recorded. Defined management ports. Student and staff VLANs defined. No documentation found for data flows. Comms between departments typically through MS Teams, 35 email or phone	Data flow must be recorded between devices. Check connection speeds/ types, port numbers, port security, firewalls. Ideally a network architecture diagram with intent. Use of MS Teams may be suitable for a smaller organisation, providing it is in line with Acceptable Use policy
ID.AM-4.	SaaS are all recorded with dates, contracts, verified users/ logins, version types. Microsoft 365 services, the primary communication and storage are accounted for. Windows Server updates are frequently recorded and checked when installing a significant change to the system. Testing here recommended, if feasible. Similar to previous suggestions, an automated tool to process log changes and security issues for all external software to ensure they are logged and in accord with policies. Ensure cataloguing of services is accessed by verified users.
ID.AM-5. Criticality based on Asset Management doc. Servers taking priority, followed by access points & switches, then printers and PCs as physical assets. Software is based on its access to critical info.	The Data Classification policy must be updated regularly, ensuring all assets are correctly classified using the 4 types of data classification.
ID.AM-6. Cybersecurity roles are established with stakeholders, however not fully defined. Leadership roles are clear, employees are not.	Clearly define security roles, particularly in IT.

Business Environment

Business Environment (ID.BE): 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.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**Yes**
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**Yes**
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**Yes**
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**No**
	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)	**No**

Results	Suggestions & Recommendations
ID.BE-1. The named organisation is a Higher Education Institute, defined by the Ministry of Education by the Dail. The Dail recognizes named organisation as it provides annual funding & supports QQI registers.	
ID.BE-2. See ID.BE-1	
ID.BE-3. Business Plan details priorities for organizational mission, objectives, and activities are established and communicated. This plan has revision and guidance from the Department of Education.	
ID.BE-4. Critical functions for delivery are not communicated clearly between departments i.e. maintenance and their policies	Ensure all parties are briefed with highlighted roles in contracts.
ID.BE-5. The two main critical infrastructure backups are reliant on the backup server found on-site. Currently only redundancy is through imaging. Online services are reliant on HEAnet for service and Microsoft 365 for mail server and backup.	Increased use of failover and implement more options for backup redundancy e.g. utilising RAID and mirror backups through virtual machines/ Contingency plan in place, not clearly communicated to those included in plan.

Governance

Governance (ID.GV): 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.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	**Yes**
	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	**No**
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**No**
	ID.GV-4: Governance and risk management processes address cybersecurity risks	**Yes**

Results	Suggestions & Recommendations
ID.GV-1. Organizational cybersecurity policy is established and communicated. Policy is not separate, integrated into other policies.	Cybersecurity policy is reviewed by board, committee understands significance, maybe more resources available to them to understand certain cybersecurity technical terms i.e. a glossary.
ID.GV-2. Roles & responsibilities are not managed and managed with clear rules or guidance. Roles are outlined, but tighter control is needed. No dedicated security team – implemented later in the organisation's life. No testing of resources as roles do not define this.	Roles are too loosely defined, many cybersecurity roles are secondary roles. Clearly define the roles, organise legally through contractual means. Resources to aid these roles through line manager. Ensure resources to improve security are recorded and treated with more importance. These will affect some subcategories in response and protect also.
ID.GV-3. Some cybersecurity regulations are understood, currently in effort to align with them, particularly GDPR. Awareness and training in place for GDPR. Data Protection Officer works with IT Dept. Licenses and contracts are documented, managed and protected.	Collaborative effort from Human Resources and IT to ensure training and awareness to ensure compliance of legality in cybersecurity. Introduction of Clean Desk policies to include for work-from-home environments, difficulties enforcing it. This may be tackled with use of timeouts and use of VPNs for critical materials.
ID.GV-4. Governance and inclusion of cybersecurity as risk management within the board of directors had been major priority for recent developments for named organisation.	See NIST SP 800-53 for further reading for further maintained compliance

Risk Assessment

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

Results	Suggestions & Recommendations
ID.RA-1. New assets are updated as soon as they are acquired. Assets that become outdated are recorded and kept on watch, considering risk tolerance.	Revise Risk Assessment and update accordingly.
ID.RA-2. As mentioned before, those at the role of cybersecurity are well-versed in up-to-date news on threats.	Revise Risk Assessment and update accordingly. Additionally, create a formal group chat for threat-related topics.
ID.RA-3. Named organisation mentioned the successful communication they have with external contacts.	Revise Risk Assessment and update accordingly.
ID.RA-4.	Revise Risk Assessment and update accordingly.
ID.RA-5. Risk assessment, risk management and risk appetite all accounted for.	Revise Risk Assessment and update accordingly.
ID.RA-6.	Revise Risk Assessment and update accordingly.

Risk Management Strategy

Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**Yes**
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	**Yes**
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	**No**

Results	Suggestions & Recommendations
ID.RM-1. The HEI had developed a Risk Management Framework document to adjust to the COVID-19 period.	Ensure all those involved are aware of the risk management processes with yearly and quarterly reminders. Users covering use of more risk-averse assets to receive training and to maintain reports to document compliance.
ID.RM-2. Board of executives have had discussions during risk assessments and are aware where the risk tolerance is. Awareness of legacy controls and how to manage that effectively.	
ID.RM-3. Noted during the audit, while risk tolerance had been established, ID.RM-3 had not been completed. Mentioned as a work in process, the correlating policies were only being developed to accommodate this relatively new risk management process, meaning it unable to conclude its role within the critical infrastructure correctly.	Complete risk management framework adjustments to fully appease the NIST framework. Ensure communication during assessments for risk management by approving and developing policies in accordance.

Supply Chain Risk Management

Supply Chain Risk Management (ID.SC): 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.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**No**
	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	**Yes**
	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.	**No**
	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.	**No**
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	**No**

Results	Suggestions & Recommendations
ID.SC-1. The benefit of being an HEI means	Please follow this publication: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf
ID.SC-2.	Document and maintain a Supply Chain Risk Assessment policy and ensure details are up to date and match each.
ID.SC-3.	Assume any contract-less partnerships are to be rectified with official documentation.
ID.SC-4.	Effort to communicate with suppliers and third-party partners to provide proof of these audits. Communicate the need for continued partnerships to include these within your risk assessment as essential assurances. Document and maintain a Supply Chain Risk Assessment policy.

	Project scope, objectives, and risks highlighted to suppliers.
ID.SC-5.	See ID.SC-4. Continue to develop and improve Supply Chain Risk Assessment. Suppliers and third-party are to be in close contact and notify when changes are present.

Protect

Identity Management Authentication and Access Control

Identity Management, Authentication and Access Control (PR.AC): 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.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**Yes**
	PR.AC-2: Physical access to assets is managed and protected	**Yes**
	PR.AC-3: Remote access is managed	**Yes**
	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	**Yes**
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	**Yes**
	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	**No**
	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)	**Yes**

Results	Suggestions & Recommendations
PR.AC-1. A formal policy outlining roles and responsibilities of users**.** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	
PR.AC-2. IT and Maintenance work in tandem to ensure physical IT assets are secured and checked daily. Users with access are briefed and recorded.	
PR.AC-3. Remote Access is managed using VPNs with limited access and briefed users. Users are recorded and given limited, only essential access	
PR.AC-4. Permissions granted to every user through Active Directory & other services.	

All users sorted via hierarchy. Hierarchy is determined by sensitivity of info that users have access to.	
PR.AC-5. Network is segregated from students and staff using separate VLANs. Students and guests access on premises via a protected wireless network.	Eduroam is a useful tool for HEIs to allow students to connect wirelessly on a segregated network linked to their student credentials. This can be accessed by any student registered with eduroam.
PR.AC-6.	See PR.AC-5 as mentioned for use of HEAnet & eduroam. Eduroam will allow a segregated and protected network, particularly for student users, but also allows credentials to be bound and proofed in interactions. Users can be managed and dealt with internally through these logs.
PR.AC-7. Wireless network is authenticated via WPA2-Enterprise. Network is monitored for uncommon behaviour.	

Awareness and Training

Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**No**
	PR.AT-2: Privileged users understand their roles and responsibilities	**No**
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	**Yes**
	PR.AT-4: Senior executives understand their roles and responsibilities	**No**
	PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	**Yes**

Results	Suggestions & Recommendations
PR.AT-1. Awareness is present but training is not. Workshops are provided but are optional.	Policy required to include cyber training as a part of HR briefing for new employees. Training should outline essentials; roles and responsibilities of users and privileges given.
PR.AT-2. On average, privileged users have more awareness and understanding of responsibilities, however lack of training does not satisfy PR.AT-2	See PR.AT-1 for suggestions. Privileged users must be briefed with training and awareness. Ensure they are organised as such.
PR.AT-3. T-parties have ensured the HEI in their training and awareness.	
PR.AT-4. Senior executives are aware of importance of their roles and responsibilities, however	Roles and responsibilities must be clearly expressed. Inclusion of Security & Training Policy to enforce compliance.
PR.AT-5. Roles and responsibilities are outlined in hiring process for cybersecurity personnel. Links back to the issue of awareness and training for other users.	

Data Security

Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	**Yes**
	PR.DS-2: Data-in-transit is protected	**Yes**
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**Yes**
	PR.DS-4: Adequate capacity to ensure availability is maintained	**No**
	PR.DS-5: Protections against data leaks are implemented	**No**
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**No**
	PR.DS-7: The development and testing environment(s) are separate from the production environment	**No**
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	**No**

Results	Suggestions & Recommendations
PR.DS-1. An incomplete risk assessment and related policies mean data isn't properly defined. However, data is protected within the risk appetite of the HEI through third-party means.	https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/ NIST.SP.800-175Br1.pdf - consider the following. Procedures to describe and record the encryption process for manual encryption/ dedicated encryption wizards grants the named HEI more control over its data.
PR.DS-2.	See PR.DS-1 and https://nvlpubs.nist.gov/nistpubs/ SpecialPublications/ NIST.SP.800-175Br1.pdf While VPN is utilized for sending and managing sensitive data remotely, utilisation of SSL/TLS encryption may enable the HEI for more secure HTTP
PR.DS-3. Access Control is a defined policy that includes handling of data and assets.	A document highlighting how to perform each task of removal, transfer, and disposition to train privileged users quicker.
PR.DS-4. Capacity is not accurately monitored, therefore no evidence satisfying the capacity amount needed.	Document the amount of total capacity from both internal and external perspectives. Allow for scaling possibilities. Test and record results to manage load amount during high-stress times.
PR.DS-5. The HEI has no data leak protection solution.	Suggest performing an audit on services that data is sent on e.g. filesharing on Teams and Onedrive https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide Microsoft provides an in-depth and updated doc with all resources, including plan for building DLP plans, processes and policy
PR.DS-6.	Refer to NIST SP 800-53. Utilise integrity verification tools to detect anomalies and unsavoury behaviour and data in your software and firmware. Highly-rated data integrity solutions include Ofni systems and Nakisa. Ensure software follows GDPR regulations.
PR.DS-7. No policies to confirm this. Student Services use a test environment separate to their live environment but find their provider do not allow much freedom when customizing it.	Implement fully functioning test environment. Ensure it is separate to the live, production environment.
PR.DS-8.	Consider risk assessment on hardware that is unmonitored and unverified. Hardware manufacturers contacted and documented.

Information Protection Process and Procedures

Information Protection Processes and Procedures (PR.IP): 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.	**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)	**No**
	PR.IP-2: A System Development Life Cycle to manage systems is implemented	**No**
	PR.IP-3: Configuration change control processes are in place	**No**
	PR.IP-4: Backups of information are conducted, maintained, and tested	**No**
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	**No**
	PR.IP-6: Data is destroyed according to policy	**No**
	PR.IP-7: Protection processes are improved	**No**
	PR.IP-8: Effectiveness of protection technologies is shared	**No**
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**No**
	PR.IP-10: Response and recovery plans are tested	**No**
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**No**
	PR.IP-12: A vulnerability management plan is developed and implemented	**No**

Results	Suggestions & Recommendations
PR.IP-1.	Create and maintain a document of baseline configurations. Ensure baseline configurations are protected documents. Limited access to the system and privileged users must be secured on the domain. This can be configured in the Active Directory
PR.IP-2.	See NIST SP 800-53
PR.IP-3.	See NIST SP 800-53
PR.IP-4.	
PR.IP-5. Mentioned the COVID-19 period introduced the Bring Your Own Device (BYOD) policy made completing this subcategory very difficult.	Clearly define the physical operating environment for work-from-home users and ensure it meets Risk Assessment policy
PR.IP-6.	Policy is not properly defined.
PR.IP-7.	Policy is not properly defined.
PR.IP-8.	
PR.IP-9.	Create an Incident Response plan that includes metrics, employees involved and their roles.
PR.IP-10.	Ensure the response and recovery plans are tested on a relatively regular basis, including new technologies that may have been introduced to your Risk Assessment Plan
PR.IP-11.	
PR.IP-12.	A vulnerability management plan is not properly defined.

Maintenance

Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	**No**
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**No**

Results	Suggestions & Recommendations
PR.MA-1. IT Team responsible for maintenance in tandem with Building Maintenance team. No accessible documents to appease this.	Document and communicate maintenance processes to relevant line manager. Revise GDPR for when handling hard drives of students and staff. Ensure Data Deletion policy is clearly communicated to users for when repairing user machines. Hard drives are removed from machines being reused. All profile data is cleared each time machines are admitted back into IT
PR.MA-2. No accessible documents to appease this.	Remote maintenance is virtually unused in the named HEI. Policy to be developed and detailing potential use if feasible.

Protective Technology

Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**No**
	PR.PT-2: Removable media is protected, and its use restricted according to policy	**Yes**
	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	**No**
	PR.PT-4: Communications and control networks are protected	**Yes**
	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	**No**

Results	Suggestions & Recommendations
PR.PT-1. Visible effort to employ these audit/logs, no formal policy is complete to satisfy this subcategory. Critical system updates and vulnerabilities are noted on WSUS, which is monitored daily.	Complete and maintain policy for audit/log recording. Events are to be recorded (type, time, info)
PR.PT-2. Outside USBs are not permitted, must be lent to users from IT department.	Removable media is protected, and its use restricted according to policy. Policy disallows outside use of removal devices. For some are permitted but ensure scanning for vulnerabilities is in place.
PR.PT-3. Principle of least functionality is not clearly defined.	The principle of least functionality is applied to users in the domain, but his definition is not clearly defined. Ensure a policy, preferably Access Control, documents this as a scope to compare this to.
PR.PT-4. Utilisation of HEAnet network for staff and students. Documented testing and reports of security provided.	
PR.PT-5. Server snapshots are included but do not include appropriate resilience.	Backup server for resilience must be tested and documented for failover for regular times to ensure it works effectively for crucial times.

Detect

Anomalies and Events

Anomalies and Events (DE.AE): Anomalous activity is detected 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	**Yes**
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	**Yes**
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors	**No**
	DE.AE-4: Impact of events is determined	**No**
	DE.AE-5: Incident alert thresholds are established	**No**

Results	Suggestions & Recommendations
DE.AE-1. Baseline of network operations are managed with control over boundaries to your perimeter network. Documented devices and what is/isn't allowed through them.	
DE.AE-2. Wireless network has built-in monitoring software that detects anomalies hardware-side. HEAnet reports anomalies and has contact in regard to events server-side. Third-party aid for determining issues found.	
DE.AE-3. Mention of using Splunk and prices quoted to begin services. Nothing in place other than manual analysis for events.	Suggestion to use Splunk, a SIEM solution. Event management capabilities from Splunk can be spread across to multiple sources and provide event logs. Document event data to compare with other event reports and other monitoring info. Analyse events and compile reports to increase ability to recognize anomalous behaviours.
DE.AE-4.	Ensure Contingency Plan, incident handling capabilities and Risk Assessment all identify and prepare for impact of events
DE.AE-5.	See DE.AE-4

Security Continuous Monitoring

Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**Yes**
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	**Yes**
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**Yes**
	DE.CM-4: Malicious code is detected	**No**
	DE.CM-5: Unauthorized mobile code is detected	**No**
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**Yes**
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**Yes**
	DE.CM-8: Vulnerability scans are performed	**Yes**

Results	Suggestions & Recommendations
DE.CM-1. Manual monitoring is currently in place. Automated monitoring alerts are in place.	
DE.CM-2. All outside personnel are recorded in and out of the building, must be accompanied by verified member if use of any devices is involved. Cameras and monitoring is in place.	
DE.CM-3. See DE.CM-2. Personnel details are recorded at reception before entry to premises. No access to physical assets without permission.	
DE.CM-4.	Consider investing in code obfuscation tools to detect malicious code activity. This can be performed on software, email downloads, portable storage devices to ensure they are safe for users. Code obfuscator may also work to scan and alert administrators to perform whatever removal or protection needed.
DE.CM-5.	See NIST SP 800-53. Define clearly acceptable mobile code & mobile code technologies.

	Analyse and monitor use of mobile code in the network and compare in Risk Assessment
DE.CM-6. HEAnet provides transparent reports and updates of anomalous events	
DE.CM-7.	
DE.CM-8. Antivirus includes vulnerability scans. Performed on every user-issued machine	

Detection Processes

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**No**
	DE.DP-2: Detection activities comply with all applicable requirements	**No**
	DE.DP-3: Detection processes are tested	**No**
	DE.DP-4: Event detection information is communicated	**Yes**
	DE.DP-5: Detection processes are continuously improved	**No**

Results	**Suggestions & Recommendations**
DE.DP-1.	Clearly define roles and responsibilities for personnel involved in detection process.
DE.DP-2.	See NIST SP 800-53 Evaluate control assessment plan i.e. describe scope of control under assessment, determine effectiveness of control, determine assessment team and environment
DE.DP-3.	See DE.DP-2
DE.DP-4. Updated list of personnel due to receive event detection information	
DE.DP-5.	Include notes and improvements from compiled event anomalies

Respond

Response Planning

Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	**No**

Results	Suggestions & Recommendations
RS.RP-1.	Incident Response Plan needs to be better developed. Consider including the following and define; - Incident Identification - Resources - Personnel, Roles, and Responsibilities - Detection, Monitoring and Analysis - Containment - Recovery - Improvements Consider testing and emulating the Incident Response Plan to ensure all phases are functional for a real incident

Communications

Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**No**
	RS.CO-2: Incidents are reported consistent with established criteria	**No**
	RS.CO-3: Information is shared consistent with response plans	**No**
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	**No**
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**No**

Results	Suggestions & Recommendations
RS.CO-1. Partially completed. Acting CISO understands his position, requests assistance from 2 other IT staff. Roles not clearly defined.	Define roles clearly within Incident Response Plan and define order of operations Expanding further **on** RS.RP-1
RS.CO-2.	See NIST SP 800-15 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
RS.CO-3.	Information sharing mentioned in https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf Outline the scope for sharing routines and processes involved. Ensure to create a trust relationship within information sharing groups is built and maintained. Allow organisation to document events openly and share them within sharing circles.
RS.CO-4.	Incident Response to be in sync with current relevant stakeholders. This may include; -board members -system owners -human resources -security & maintenance

RS.CO-5.	Information sharing mentioned in https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Analysis

Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**Yes**
	RS.AN-2: The impact of the incident is understood	**Yes**
	RS.AN-3: Forensics are performed	**No**
	RS.AN-4: Incidents are categorized consistent with response plans	**Yes**
	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)	**No**

Results	Suggestions & Recommendations
RS.AN-1. Use of Windows Event Log manager for AD issues, Windows 365 Admin Centre for the mail and online data storage logs. Miraki gives monitoring updates with event logs for the HEI's WFi detection.	
RS.AN-2. The impact of the incident is understood	
RS.AN-3.	See NIST SP 800-72 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-72.pdf Discusses use of PDA tools for the use of performing forensics. The document also discusses how to report your findings correctly. This will lead back to the compliance of data sharing in RS.CO-3.
RS.AN-4. The current Incident Response Plan has categorisation, as stated by NIST, in 4 different levels; low, mid, high, critical.	Ensure categorizations are consistent with data type and platform found on e.g. email, file sharing, security apps, networks data
RS.AN-5.	See NIST SP 800-72 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-72.pdf

Mitigation

Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-1:** Incidents are contained	**Yes**
	RS.MI-2: Incidents are mitigated	**Yes**
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**No**

Results	Suggestions & Recommendations
RS.MI-1. As mentioned by NIST, a Containment Phase is comprised of short-term, long-term and backup. Evidence of a Containment Phase is documented. Backups are verified and logged.	
RS.MI-2. As mentioned by NIST, a Mitigation Phase is comprised of metrics of the time an incident occurred, the number of incidents, a description of the damage and attempt.	
RS.MI-3.	Include in Vulnerability Management policy how to effectively mitigate and contain incidents.

Improvements

Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	**Yes**
	RS.IM-2: Response strategies are updated	**No**

Results	Suggestions & Recommendations
RS.IM-1. Response plans are built upon previous attacks and compiled data sharing notes	
RS.IM-2. No evidence of strategies being updated regularly	Strategies must be updated recently, define in Incident Response Strategy how often these are to be updated and note formally when you do. E.g. every 2 months, ad hoc

Recover

Recovery Planning

Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	**Yes**

Results	Suggestions & Recommendations
RC.RP. Recovery plan is executed during or after a cybersecurity incident	

Improvements

Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**Yes**
	RC.IM-2: Recovery strategies are updated	**Yes**

Results	Suggestions & Recommendations
RC.IM-1. Recovery plans incorporate lessons learned. Incident Response Plan is updated on a bi-monthly basis to ensure it is in line with assessed changes in Vulnerability Management Policy	Perform tests for Recovery Plan to ensure it is effective in a live environment
RC.IM-2. Recovery strategies are updated bi-monthly and for every significant change that affect the Recovery Plan	

Communications

Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centres, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-1:** Public relations are managed	**Yes**
	RC.CO-2: Reputation is repaired after an incident	**No**
	RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	**No**

Results	Suggestions & Recommendations
RC.CO-1. President of named HEI is aware of role to be spokesperson for incidents during and post-recovery. Human Resources and Head of IT have outlined response as part of Incident Response Plan	
RC.CO-2.	Recovery time is essential to reputation for an organisation, so ensure you are performing tabletop exercises to emulate incident response and incident recovery to allow an estimated time to communicate to all involved.
RC.CO-3.	See RC.CO-2

Final Results

Identify	ID.AM	3/6
	ID.BE	3/5
	ID.GV	2/4
	ID.RA	6/6
	ID.RM	2/3
	ID.SC	1/5
Protect	PR.AC	6/7
	PR.AT	2/5
	PR.DS	0/8
	PR.IP	0/12
	PR.MA	0/2
	PR.PT	2/5

Detect	DE.EA	2/5
	DE.CM	6/8
	DE.DP	1/5
Respond	RS.RP	0/1
	RS.CO	0/5
	RS.AN	3/5
	RS.MI	2/3
	RS.IM	1/2
Recover	RC.RP	1/1
	RC.IM	1/1
	RC.CO	4/6

Results	**Yes**	**47**
	No	**59**
	Total	**106**

As seen by the results of the audit, the named HEI had scored 47/59. This scoring system is designed to understand how closely your subject meets the NIST expectations, and the subcategories score shows where the subject is particularly weak.

Identify scored a total of 17/29. The named HEI shows strength in the Risk Assessment element of this function, having scored full marks. This shows the HEI's strengths in its risk awareness and its process of Risk Assessment. Having spoken to a member of IT staff in the named HEI, they had mentioned that risk was something they had been moving their focus towards in recent months, specifically for the hybrid learning model the majority, if not all HEIs had undertaken during the COVID-19. As mentioned, and predicted by my previous research, the shift of business operations to almost exclusively online has given less overall retention to HEIs, so cyberattack of any type that may slow, or halt business operations may have a larger affect than under usual circumstances.

The Supply Chain Risk Management showed shortcomings in the supply chain, with a theme of unestablished and unidentified contracts with suppliers & third-party entities. The next course of action to rectify this would be to list every third-party point of contact and run through the framework again.

Protect scored the lowest of the functions with 10/39. The named HEI seemed to be successfully achieving asset management, however falls short in the PR.DS and PR.IP sections. This leads you to believe that the documenting and maintaining of policies seems to be lacking in this particular HEI's case.

Detect scored a 9/18, which the Continuous Monitoring section taking a lead in this function.

Respond managed a 6/16, having shortcomings in the Communication settings. Judging by this, the HEI had not fully established the roles for internal and external players involved in the response planning.

Recover completed a 6/8, a strong score for this section.

Further Comments

The notable effectiveness of the NIST CSF Audit is how binary it is; its either compliant or its not. This is ideal for the likes of a research project, that benefits from results that are tangible; stats, data, numbers. However, an important part of research is the primary sources that you obtain from conversation and attitudes noticed and exhibited from those operating on the ground every day.

Risk Assessment

Looking at the successes measured by the audit, one of the most noticeable

Part 3 – NIST-Based Cybersecurity Survey

Survey Overview

The Cybersecurity Readiness Survey was originally the primary element of this final project. The survey comprises of 22 NIST-based questions designed to be answered by HEIs to give an insight into how they are operating cybersecurity-wise. Once the results were compiled, they would be used to compare against the others to give a general idea of how all HEIs were doing in comparison to each other. The questions follow the NIST framework, remaining relevant to the initial direction proposed by the project.

This survey is based on the research conducted in the initial research stages of this project. They consisted of varying types of surveys and questionnaires from different organisations aimed at their employees and customers.

This survey was sent out to a total of 10 HEIs. The users contacted were the members of the IT staff of each organization. Using the online resources found on the corresponding HEI's website, a list was compiled, and the contacts were prompted to answer the survey.

Survey Questions

Please see Table of Figures to see the Cybersecurity Readiness survey questions. The screenshots FIG 1 through 17 show the disclaimer and the 1 survey questions.

Survey Results

The survey yielded the following results from 3 separate HEIs that answered. These results are as follows.

	HEI #1	**HEI #2**	**HEI #3**
1	Yes, board member	Yes, reports to board	No
2	Yes	Yes, not updated	Yes, not updated
3	Yes	No	No
4	SIEM Software, HEAnet	SIEM software, HEAnet	HEAnet
5	Miraki Wireless	N/A	N/A
6	Ad hoc	Ad hoc	Ad hoc
7	Servers, APs, Software, SaaS	Network Perimeter, Servers, APs, Devices	Servers, APs, Devices
8	Both	Both	Neither
9	Sometimes	Sometimes	Sometimes
10	Yes, Staff only	Both	Yes, Staff only
11	No	No	No
12	No	Yes	No
13	Yes	Yes	Yes
14	Yes, but there is more work to do.	Yes, we have been moving forward to meet the challenges of the online	Yes. The process of securing

		landscape. Still working towards safer and more secure systems.	
15	A major security challenge found during the transition was the assessment of risk management and how to define that. Having your organisation online has changed the scope of risks and having to rely more on policy and trust from employees have changed risk factors significantly.		
16	I would say cybersecurity has taken a priority. The NCSC has been lending its expertise to the Dept. of Education and provide very useful guides in the past couple of years.	I believe the priority for cyber security has become a priority for all affected Irish departments, and as a result, tertiary level institutions have benefited from this increased level of attention.	I think cybersecurity has become more focused on by the Irish government in general, however

As seen by the results, there are mixed results from the different submissions. The variation between each HEI is not immediately apparent, but as the results are analysed, each HEI starts building a profile based on the answers given.

Notable Points

The main concern that came from the amount of total answers. Overall, from the 10 recipients that were contacted, only 3 responses were received. Referring to the metrics section of the functional specification document, I was anticipating at least half of the 10 contacts would respond to this survey. This would've been preferable to allow for a deeper pool of results to compare from, making it a more tested survey.

The reliance on HEAnet's systems was both interesting and somewhat predictable.

Conclusions

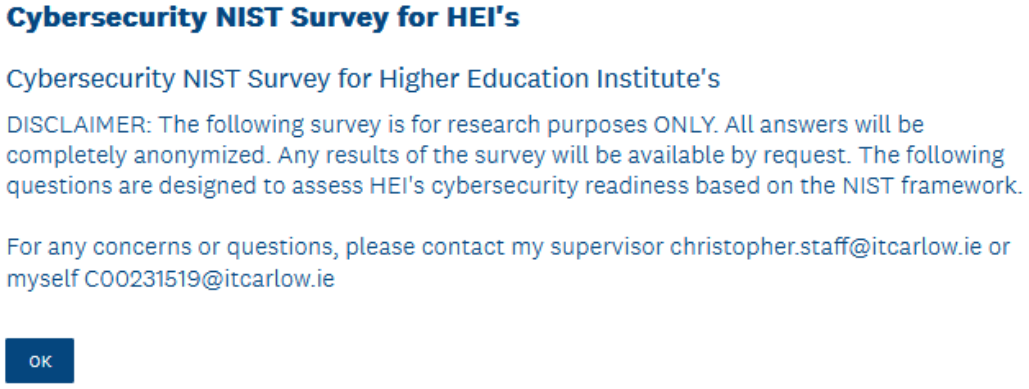
The overall conclusion to both the survey and the audit was successful.

The NIST audit was hugely beneficial in the process of uncovering a meaningful scope of capabilities possessed by the sample HEI. The audit really dove into the finer details of the HEI, specifically how it operates and how it enforces and documents the various policies and plans needed to have all bases covered in preparation for the crises that may arise in business. There were points mentioned about the COVID-19 period and how HEIs were adapting found in the NIST audit which was valuable to note for this project.

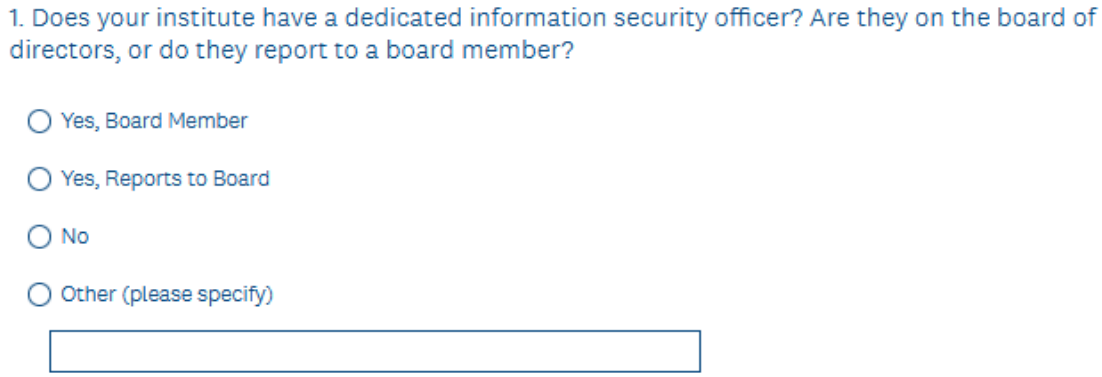
The survey did not have the same impact originally planned. With limited responses from HEIs, the survey segment was successful in execution, however the predicted responses were not as thorough as expected. To provide a stronger analysis between HEIs, a larger test audience would have been reached. Despite this, the info gathered was still relevant and useful for analysis in the project.

These survey results, coupled with the NIST audit have given a much better idea of where HEIs operate regarding their cybersecurity during the COVID-19 period.

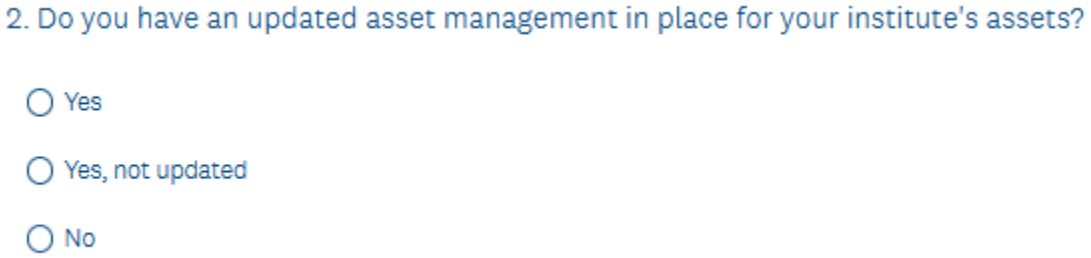
Table of Figures



[FIG1] Cyber Readiness Survey Disclaimer



[FIG2] Cyber Readiness Survey Question 1



[FIG3] Cyber Readiness Survey Question 2

3. Do you have risk management process established?

- ◯ Yes
- ◯ No

[FIG4] Cyber Readiness Survey Question 3

4. How do you monitor your institute's network?

- ◯ Security Operations Center (SOC)
- ◯ SIEM Software
- ◯ HEAnet
- ◯ Splunk
- ◯ None

[FIG5] Cyber Readiness Survey Question 4

5. What vendor do you use for monitoring?

[FIG6] Cyber Readiness Survey Question 5

6. Do you monitor systematically? Choose the answer that best suits.

- ◯ Automated
- ◯ Ad hoc
- ◯ Scheduled

[FIG7] Cyber Readiness Survey Question 6

7. What are you monitoring? Choose all that apply.

- [ ] Network Perimeter
- [ ] Servers
- [ ] Switches
- [ ] Access points
- [ ] Devices
- [ ] Software
- [ ] SaaS

[FIG8] Cyber Readiness Survey Question 7

8. Do you monitor student & staff activity on your network?

- ○ Both
- ○ Staff
- ○ Student
- ○ Neither

[FIG9] Cyber Readiness Survey Question 8

9. Does your password policy ensure your staff and students must reset their passwords often? If so, how often?

- ○ Always
- ○ Usually
- ○ Sometimes
- ○ Rarely

[FIG10] Cyber Readiness Survey Question 9

10. Do you have phishing awareness training for both staff and students?

- ◯ Yes, both
- ◯ Yes, Staff only
- ◯ Yes, Student only
- ◯ No

[FIG11] Cyber Readiness Survey Question 10

11. Do you have simulated threat response activities e.g. tabletop activities?

- ◯ Yes
- ◯ No

[FIG12] Cyber Readiness Survey Question 11

12. Do you have a vulnerability management plan in place?

- ◯ Yes
- ◯ No

[FIG13] Cyber Readiness Survey Question 12

13. Do you have a response plan for a security incident?

- ◯ Yes
- ◯ No

[FIG14] Cyber Readiness Survey Question 13

14. Are you satisfied with your institute's response to the evolving threat landscape of hybrid/ online learning? Please explain your answer.

[FIG15] Cyber Readiness Survey Question 14

15. Have you found any major security challenges during the transition to hybrid working? More for staff or students, or both? Please explain your answer.

[FIG16] Cyber Readiness Survey Question 15

16. Do you think cyber security has become a priority for the Department of Education since the shift to hybrid learning? Please explain your answer.

[FIG17] Cyber Readiness Survey Question 16