NIST
Cyber Security Framework

Cyber Security Engineering: Governance and Management of Cyber Security ICS0009

Aleksander Tkatšenko
Anıl Yarkın Yücel 184082IVSB
Iqbal Bagaskara
Ryo Shiraishi 195557IVSB

Introduction

In response to Presidential Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” which layout the necessity to build a standardized cybersecurity framework for critical infrastructures in the United States, The National Institute of Standards and Framework released Cybersecurity Framework (CSF) in February 2014. NIST CSF is used to help many organizations to set the standard for many organizations from the public and private sector as a resource to create a secure infrastructure from the perspective of cybersecurity threat and attacks which can disrupt their service.

Our report corresponds to the implementation of NIST CSF framework in a water supply system of town having 20,000 inhabitants. Our facility has implemented a security policy that corresponds with ISO27001 standard. As our town population increases, our water facility needs to improve and grow to adapt to the demands of the town inhabitants. As an organization grows, normally the complexity of the system that we implement will also increase. Disruption to our water facility’s service could potentially disrupt the whole town and could even become dangerous as water is an essential part for people’s needs from consumption, sanitization, agriculture, etc.

This report will explain the procedures of implementing NIST CSF which includes its categories, subcategories, and tier of our security policy implementation. We take our references from several sources:

- CIS CSC
- COBIT 5
- ISA 62443-2-1:2009
- ISA 62443-3-3:2013
- ISO/IEC 27001:2013
- NIST SP 800-53 Rev. 4

Identify Function

Asset Management (ID.AM)

That is obvious that a water supply company will not have a lot of devices, either end-user devices, like computers, storage devices, and peripherals, or networking units like routers and switches, yet it is important to avoid any disruptions in the work of a water supply company. Therefore I consider it being highly vital to have strict and complete asset management. This is not going to be hard to implement because there are not many devices that need to be documented and not many devices will be added in the future if any.

- ID.AM-1: Physical devices and systems within the organization are inventorised
  This should already be implemented by ISO 27001 as per A.8.1.1, all present within the organization devices and systems should be documented, their characteristics, their version or model as well as a unique identifier if present. MAC addresses for NICs on computers and other network units. For computer peripherals to document their VID and PID (vendor ID, product ID). All information should be updated

according to all sorts of events, creation of the new device, processing, storage, transmission, deletion, or deconstruction.
A water supply in particular mostly consists of mechanical elements such as valves, pumps, pipes, water tanks and filters. But in order to ensure consistent work of the whole system we turn to electronic devices for help, and this is where cybersecurity comes into play.
Here is the brief overview of electronic devices that may appear in a water supply system: mostly various sensors (water level, pressure, temperature, amount of air and other water components), logging, storing and monitoring devices, cables or other means of distant communication. Personal or work devices of employees. Besides that, pumps and valves can be manipulated by electric means, either automatically or manually. A computer that makes various decisions whether to close a valve or not, etc.
All of this is considered assets and should be documented.

- ID.AM-2: Software platforms and applications within the organization are inventoried
  This should also have been implemented by A.8.1.1, where all software should be documented in very little detail. Starting with the name of the software/application, version, date, and location of download, as well as on what devices this software is installed. Any new software should also be added to the list. After removing some software, even if no devices use it, information about it should remain, in case we will need to install it back we will know exactly what version to install, or in case this software has damaged any devices we will be able to pass this software to a professional who will be able to provide a proper way to restore from that damage. Documenting assets does not require any expenses and does not take much time. For a water supply each asset might include its own software, and all of those should be documented.
- ID.AM-3: Organizational communication and data flows are mapped
  Referred to as A.13.2.1, A.13.2.2, all the communication and data flow should be documented, from where to where the information goes, especially in places where information leaves the organization to third parties. As per ISO 27001, all this is already implemented and no other actions are required.
  For a small water supply, most reasonably is to have everything centralized, all data from sensors should come to one single computer, where it will be stored and processed. Only certain, specific data is allowed to be transferred beyond that computer. This includes, but is not limited to, water pressure at end-users, water chemical components, amount of bacteria and other information that must be publicly available by legal policies.
- ID.AM-4: External information systems are cataloged
  Most often all cyber threats come from outside of the organization, therefore it is vital to document external information systems that this organization interacts with. ISO 27001 A.11.2.6 also documents all off-site equipment and assets, therefore external systems should be already cataloged.
  A small, but not so much, water supply is able to handle all work on its own, therefore not many external information systems are used, but it might use the following: email service, cloud storage for backups and other quality of life services.
- ID.AM-5: Resources are prioritized based on their classification, criticality, and business value

In addition to A.8.2.1 we should also document what resources of this organization are the most important to their business environment, in other words, which resources make the most money. It is also important to note which resources are more critical and which are less, this way we will have a clear picture of what resources to prioritize our focus. Without this information, all the actions to reduce risk will be less cost-effective. Constructing such a document could take some time because it requires evaluation of all resources and their roles within the organization. Obviously that one central computer that we talked about earlier is high priority because it controls everything and includes all the data, and can be considered as a single point of failure. Next priority is sensors, they ensure that everything is working consistently, therefore it is important that no one can temper with them.

- ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established
  With A.6.1.1 all information security responsibilities are already defined and allocated among parties. Besides that, from time-to-time, those roles and responsibilities must be rescaled because the supply chain changes gradually over time and it might require a complete re-evaluation of roles and responsibilities to ensure that they are distributed and established the most effective way possible. Implementing this control may require huge expenses depending on whether the existing workforce has the necessary skills and time for handling specific roles and responsibilities of cybersecurity, in the worst case this will require hiring specific professionals.
  A water supply isn't anyhow related to cybersecurity therefore I think there is no other way than hiring a specialist, who is going to be responsible for defining and managing all cybersecurity processes.

Business Environment (ID.BE)

- ID.BE-1: The organization's role in the supply chain is identified and communicated
  This subcategory is fully covered by ISO 27001 Annex 15. All the relationships and agreements are established. The organization has a complete understanding of its role in the supply chain. As for a water supply system it is crucial to understand its importance and effect on its supply chain because it has many interactions with third parties. Whether a factory, a farm or a residential area, they all greatly depend on a reliable source of water, therefore it is vital that a water supply meets their needs.
  A water supply surely belongs to an enormous supply chain. A decent amount of paperwork and negotiating must be done before the whole supply chain will be fully identified.
- ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
  Not many organizations belong to critical infrastructure, but a water supply certainly does. Disruptions in work of a water supply causes damage to the whole town, this is for sure. But this might lead to disruptions in work of even more critical infrastructure elements that could case damage of a national-wide level.
  Imagine a situation where a nuclear power plant will run out of water to cool down their reactors? Or a whole harvest will die out because of a sunny day?

Such things could happen in an instant, but could cause irreversible damage over an extended period of time.
It is extremely important for a water supply to always take into account its crucial effect on a whole infrastructure and always proceed with caution.
This topic is well described by ISO 27001 Clause 4.1.

- ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
  This subcategory ensures the organization focuses on its goal. It is not covered by ISO 27001, therefore, needs to be done from scratch. For a water supply organization, it is highly important that everyone has access to water and it is also important that there are no disturbances. But it is also vital that the quality of water is acceptable and pressure is good enough so that the water could get to most distant customers.
  Without a clear view of organizational objectives, it is impossible to appropriately calculate the risks associated with organizational activities. In our case, the most important objective is that all customers have constant access to water therefore anything that could cause disturbances in supplying water should be considered as a high priority.
- ID.BE-4: Dependencies and critical functions for delivery of critical services are established
  This subcategory is greatly covered by ISO 27001 A.11.2.2, A.11.2.3, A.12.1.3.
  The goal of this subcategory is to identify and document what assets are the most important to delivery of the service, in our case the following assets can be considered as the most important: source of water (such as lakes and underground rivers), filters, water storage, pipes and pumps. These are the assets that the organisation must focus on.
- ID.BE-5: Resilience requirements to support the delivery of critical services are established for all operating states
  This category is well covered by ISO 27001 A.17.1 ensuring that service can continue its work under any condition.
  What means even if something causes the service to degrade, the service will be able to continue to work even in that state, and will not collapse all together.
  In example: there are two pumps at a water storage, if one of them goes out of order that means the service is operating at 50% of its base capability. Repairing a pump takes time, and we should ensure in advance that even if one of the pumps breaks the other one will be able to withstand the increased pressure. Otherwise while we repair that broken pump the other one will also break. Leading us to a 0% of service.

Governance program (ID.GV)

- ID.GV-1: Organizational cybersecurity policy is established and communicated
  In this subcategory we ensure that an organizational information security policy does exist and is maintained. And do the employees and relevant external parties know and follow this policy.
  Should be already implemented according to ISO 27001 A.5.1.1.
  In our case, on a water supply, there is no need for complex policies. An employed cybersecurity specialist knows his stuff so there is no need to explain anything on his

end. But for other employees, rules are simple: do not touch the central computer, do not record to their personal devices any data related to a water supply.

- ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
  This subcategory states that all cybersecurity responsibilities should be distributed between internal workforce and third parties, ensuring that no assets are left without protection. Whether there is a cybersecurity team or a carpenter, roles and responsibilities should be understood and maintained.
  This has been covered and implemented by A.6.1.1 the same as ID.AM-6.
  In case of a water supply, all of the cybersecurity responsibilities go to the cybersecurity specialist.
- ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
  This subcategory is in-depth described by a whole A.18 covering from the identification of applicable legislation and contractual requirements to the regulation of cryptographic controls.
  Being a part of a critical infrastructure, a water supply has many legal and regulatory requirements to follow, therefore a well documented and repetitive procedure must be established.
- ID.GV-4: Governance and risk management processes address cybersecurity risks
  Cybersecurity risks should be treated as the organisation-wide risks because they can easily pile up and completely wipe out the organisation.
  Covered by ISO 27001 clause 6.
  In a water supply were not much but very vital assets, it can be considered as a high priority to address cybersecurity risks on an organisation-wide level.

Risk Assessment (ID.RA)

- ID.RA-1: Asset vulnerabilities are identified and documented
  There should be a complete documentation on vulnerabilities on previously inventoried assets (ID-AM1). Without knowing weak spots of the organisation it is impossible to protect it efficiently. This information is helpful for both Protect and Detect functions.
  Covered by A.12.6.1, A.18.2.3.
- ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
  Besides reading news and forums regarding cyber threats I would recommend also stay informed regarding possible acts of terrorism, either civil or politic based, because a water supply company quite likely could become a target for such an event.
- ID.RA-3: Threats, both internal and external, are identified and documented
  Based on known vulnerabilities, possible and non negligible threats should be documented. This includes vulnerabilities that are not yet resolved or the organisation is unable to resolve.
  Done according to ISO 27001 clause 6.1.2
  There are many threats for a water supply, both internal and external, therefore it is highly important to identify and document as much of them as possible.

- ID.RA-4: Potential business impacts and likelihoods are identified
  Impact and likelihood - are the key properties of threats, based upon which threats are prioritised. These define the sequence of safeguard implementation which means that this information helps us utilize time effectively.
  The worst case scenario a water supply will go completely out of order. Therefore everything that causes not local but global disturbances must be assigned highest priority.

- ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
  This is where all the information combined gives us the final result.
  In previous ID.RA subcategories we have gathered all the necessary information for the main goal of the risk assessment category: determining the risks.
  Now that we know all risks' key components we say, with confidence, that we must put most of our effort into protecting the central computer. Protecting everything else comes after.

- ID.RA-6: Risk responses are identified and prioritized
  An extended period of time without water could cause great damage therefore for a water supply it is highly vital to be able to resolve any kind of issues in the shortest time possible.
  This subcategory is already partly covered by ISO 27001 clause 6.1.3. But I would recommend identifying all the risk responses once again as well as carefully distribute risk responsibilities and priorities because this would help to avoid any disastrous consequences.This subcategory is already partly covered by ISO 27001 clause 6.1.3. But I would recommend identifying all the risk responses once again as well as carefully distribute risk responsibilities and priorities because this would help to avoid any disastrous consequences.

Risk Management Strategy (ID.RM)

- ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholder
  In this category, all risk management processes must be accepted and controlled by stakeholders. All previously established practices should be always followed. For a water supply, whose work can be seen as simple and static at the first glance, it is hard not to forget to follow all policies and practices.
  Stakeholders should, from time to time, ensure that all policies are constantly followed and all employee's understanding of risks does not decay over time.
- ID.RM-2: Organizational risk tolerance is determined and clearly expressed
  Priority number one is properly prioritizing things. It is recommended that organizational risk tolerance is well determined and clearly expressed because it enables the organization to think saner during time crucial contingencies.
  As I previously mentioned, a water supply must never go completely out of order. People can survive a day without water, go to shower tomorrow, postone doing dishes for a while, disable backyard sprinklers for a while, drink bottled water, in other words reduce consumption of water to a minimum.

But there are certain things that cannot go without water supply, for example firefighters, nuclear power plants or farms.
Therefore a water supply, in certain circumstances, can operate just as little as 1% of its base capability but it must never go to 0% for an extended period of time.

- ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis

  The organisation should understand, if it is impacted, how it will impact others, and its supply chain as a whole.
  For a critical infrastructure element, such as a water supply, it is advisable to first take a look at accidents that already took place in the world, and those that luckily were prevented.
  Accidents such as poorly configured software on sensors, virus on an employee's laptop, unauthorized installation of unapproved software, malfunctioning sensors caused false alarm that caused anxiety and cry-wolf effects, misconfigured firewall and missing authentication process on a central computer and many similar..
  Taking into consideration these accidents we can build our own knowledge on how to protect a water supply.

Supply Chain Risk Management Strategy (ID.SC)

- ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders

  Having a well established cyber supply chain ensures durability of an organization, therefore it is vital to carefully choose suppliers and their vendors.
  In ISO 27001 this subcategory and other subcategories in ID.SC are covered by A.15.
  In the water supply system there is not much data being exchanged between third parties but any of this information could potentially be used for an attack on the water supply.
  Cyber supply chain for the water supply may include, but is not limited to: various emails between clients and stakeholders, some information of clients, anomalies in logging data.
- 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

  In this subcategory we prioritize and assess an organization's supply chain risk in order to build up clear understanding of their impactfulness on an organization.
  Having many suppliers and vendors may obfuscate the importance of each of them individually but prioritizing and assessing them makes it easier to split them into chunks or categories that are much easier to work with.

- 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

An organization must ensure that their cybersecurity policies are aligned with their suppliers' and third-party partners' contracts in order to build a strict and firm cyber supply chain program.

- 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

  This particular subcategory ensures that established contracts in the previous subcategory, ID.CS-3, are actually being used.

- ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers

  In this subcategory you ensure that your suppliers and third-party providers provide reliable service and do they rely on your services' reliability.

Protect Function

Protect function is an important part in the implementation of NIST framework. The main purpose of this function is to define safeguards for the critical infrastructure delivery. Based on the NIST example, the example implementation of this function includes Identity Management and Access Control, Awareness and Training, Data Security, Information Security Protection Processes and Procedures, Maintenance, and Protective Technology.

Implementation of the protect function requires it through a proactive approach. The manifestation of these categories and the Protect function as a whole is seen in two- and multi-factor authentication practices to control access to assets and environments and employee training to reduce the risk of accidents and socially engineered breaches. Under this category, there are five sub categories that defines more specifically the protect function:

- Identity Management, Authentication and Access Control (PR.AC)
  - Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
  - Physical access to assets is managed and protected
  - Remote access is managed
  - Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
  - Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
  - Network integrity is protected (e.g., network segregation, network segmentation)
  - Identities are proofed and bound to credentials and asserted in interactions
  - Users, devices, and other assets are authenticated

- Awareness and Training (PR.AT):
    - All users are informed and trained
    - Privileged users understand their roles and responsibilities
    - Third-party stakeholders
    - Senior executives understand their roles and responsibilities
    - Physical and cybersecurity personnel understand their roles and responsibilities

- Data Security (PR.DS)
    - Data-at-rest is protected
    - Data-in-transit is protected
    - Assets are formally managed throughout removal, transfers, and disposition
    - Adequate capacity to ensure availability is maintained
    - Protections against data leaks are implemented
    - Integrity checking mechanisms are used to verify software, firmware, and information integrity
    - Integrity checking mechanisms are used to verify software, firmware, and information integrity
    - Integrity checking mechanisms are used to verify software, firmware, and information integrity
    - The development and testing environment(s) are separate from the production environment
    - Integrity checking mechanisms are used to verify hardware integrity

- Information Protection Processes and Procedures (PR.IP)
    - A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles
    - A System Development Life Cycle to manage systems is implemented
    - Configuration change control processes are in place
    - Configuration change control processes are in place
    - Backups of information are conducted, maintained, and tested
    - Policy and regulations regarding the physical operating environment for organizational assets are met
    - Data is destroyed according to policy
    - Protection processes are improved
    - Effectiveness of protection technologies is shared
    - Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
    - Response and recovery plans are tested
    - Cybersecurity is included in human resources practices
    - A vulnerability management plan is developed and implemented

- Maintenance (PR.MA)
    - Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
    - Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access

- Protective Technology (PR.PT)
    - Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
    - Removable media is protected and its use restricted according to policy
    - The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
    - Communications and control networks are protected
    - Mechanisms

Procedure of Identity Management, Authentication and Access Control (PR.AC)
According to ISO 27001, access control, identity management, and authentication is necessary to limit access to information and information processing facilities. An organization should limit access to certain sectors of the organization to minimize the risk of unauthorized access which can harm the organization's functionality to deliver its product / service.

The first subcategory is "Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes". IWe need to keep the employee management and human resources in connection with our cybersecurity team to make sure that a certain person belongs to the correct department and given the right access, or revoked if they do not have the authority to access certain functionalities in the facility. Once the person has resigned from the position he is in, the right of access should be revoked and adjusted depending on the condition the employee is in; Resignation from the company or department shift.

The next procedure is to fulfill the subcategory of "Physical access to assets is managed and protected". Physical limitation of access to most of the facility is crucial since we have to limit unauthorized access in the facility. There are many important functions such as data centers or chemical inventories in the facility where only authorized people with secure access in a particular department are allowed to access. Physical access to assets should have proper documentation and inventoried according to rules agreed upon. Entry controls need to be selected and implemented based on the nature and location of the area being protected, as well as having it logged and documented. On top of that, we need to be ready to protect those areas from unavoidable circumstances or disasters such as natural disasters. The physical facility design and building needs to be consulted with experts who work on the field of construction and disaster recovery.

The next procedure is fulfilling subcategories "Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties" and "Network integrity is protected, segregated, and segmented to limit unauthorized access to certain networks". The procedure to fulfil it includes segregation of duties, which includes the access management to networks and network services in the facility. Each segregated position needs to have limitations of the access right that they have not only into the physical facility but also into our networks. In case there will be a need to have a remote working scenario, which might be not that necessary when it comes to physical and direct maintenance of our devices, we should make sure that the person only accesses our

network through authorized devices provided from our facility. Protection to our source code should also be monitored so that only people who have authority and those who directly work on it are allowed to access and manage it. The control of any versioning and update should also be tested separately and approved before merging it into our main source code.

Procedure of Awareness and Training (PR.AT)
Human resources are important parts and keys into our facility functionality and service. Education and training is well necessary in order to guarantee that our employees can do their job well and securely. In the context of cybersecurity, education about performing the job securely is sometimes not necessarily in the mind of employees and human resource managers especially if the person does not work directly in the area that regularly accesses our internal network or critical equipment in our facility.

The first subcategory is “All users are informed and trained”. These training are necessary so that all employees can recognize cyber attack attempts that target our facility as well as most importantly know the right and proper way to protect their working environment. These training should be carried out by the information security team partnering with HR or the Learning and Development team to create awareness, education, and training throughout the employment lifecycle and not only at the beginning or on employee’s boarding time into our organization. These training should be documented and proven to the auditor.

The next subcategories are “ Privileged users understand their roles and responsibilities” and “Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities”. Both parties have different access and authorization that most of the time are different than regular employees. Privileged users should have a comprehensive knowledge of the access granted under his authority and should be more aware of protecting these confidential information. Often, privileged users are more prone to targeting attacks such as spear fishing because of various information that can be obtained if the attacker can obtain these information from one source. On the other hand, third-party stakeholders that partner with our companies need to understand our dependability and if we grant some access for them. These access might include access to our chemical products that are commonly supplied by a third-party provider. Third-party partners should understand the procedures that we implement to protect our secure facility. An example is maintaining communication between the third party and our organization. Our partner needs to inform us if they have to change the regular delivery officer. Any new user from a third party provider should be verified by both the third party and our organization.

Procedures of Implementing Data Security (PR.DS) Category
Data security is the process to maintain organization\s data integrity, confidentiality, and accessibility. Preventing unauthorized access, data corruption, and denial of service attacks are important purposes that we want to achieve in our organization.

The first subcategories to be implemented are Data-at-rest is protected and Data-in-transit is protected. Procedures for handling assets need to be developed and implemented in accordance with the information classification scheme. For our water facility data to be protected, we need to maintain formal records of the authorised assets recipients and mapping our data access policy. Protecting data-in-transit is considered harder since our

data is dynamically moving between services. Thus, we need to implement some best practices such as implementing robust network security controls, Choosing data protection solutions with policies that enable user prompting, blocking, or automatic encryption for sensitive data in transit for example on email about sensitive files or information, and encrypt our data before being transferred using encrypted connections (HTTPS, SSL, TLS, FTPS, etc.).

The next subcategories to implement is Adequate capacity to ensure availability is maintained. Availability of access data such as log and information should be made accessible to manage problems such as troubleshooting. There are three important capacity types in capacities management; Data storage capacity to make sure that we will have enough space for our data and at the same time manage the capacity for backup procedures (Depends on our implementation and backup procedures mechanism); Processing power capacity to make sure our energy source that powers our facility's infrastructure is reliable; and Communications capacity or bandwidth to erasure that our communication network can be made in a timely manner.

The next subcategory is Integrity checking mechanisms are used to verify software, firmware, and information integrity. Guaranteeing that software having the right integration with one another is important to keep the system runs. It is also good to make sure all updates of software and firmware are tested and verified when integrated to the current system. If we have a good assets documentation including software assets, managing this subcategory will be much easier. Implementation that we can apply includes protection against malware, control management of Installing Software on Operational Systems, and limiting changes only on necessary software packages update.

The importances of our facility to provide essential needs for people in the city means that we should maintain accessibility and reliability of our service. With a continuously growing population, our facility also needs to make improvements including integration between hardware, software, and communication network. It creates a necessity for our organization to implement the subcategory of The development and testing environment(s) separate from the production environment. Changes and new developments should be thoroughly tested in a separate area before being deployed to the live operating water treatment facility that connects directly to our service. This procedure is meant to prevent failures in the testing and works as a safeguard and prevents access of our live environment from unauthorized access. Ideally, testers should not have direct access into our core live system. The auditor will be checking to see that development, test and live environments are separated and that there are formal procedures including appropriate levels of authorisation for moving changes and developments from one environment to another.

As our facility deals with physical objects and devices, checking mechanisms to verify hardware integrity is a mandatory part. It is neatly tied with our physical access management and regulation policies. Such maintenance should be done according to our third party provider's maintenance guidance. As we want to keep the accountability of our equipment maintenance, it would be beneficial to keep this data to be shown to our auditor. This record should include time, purpose of maintenance, the party who does the maintenance, and also the scheduled upcoming maintenance. When we implement the internet of things on our physical device equipment, this maintenance becomes more and more important.

Information Protection Processes and Procedures (PR.IP)

Management of policies related to security principles in our facility needs to be defined in details including its scope, roles, responsibilities, management commitment, and coordination among organizational entities. A proper policy that explains process and procedures should be maintained and used to manage protection of information systems and assets.

In the context of water facility treatment where there are a number of departments outside of the security protection department, it is important to properly map out the relation between each department and policies that they carry out. In the event of incidents for example, in the case that the information security department detects unauthorized access, information pipeline and coordination should exist to decrease the response and handling time and detect the vulnerable target in our water facility functionality after the attack.

The procedure of implementing subcategories " A System Development Life Cycle to manage systems is implemented" is quite huge. Taking references from CIS CSC 18 standards, we can implement these requirements in our software development lifecycle implementation in our facility; Establish Secure Coding Practices and suring error checking for our in-house developed software which is quite common to adjust the needs of specific infrastructure that applies in our facility; Verifying the software we used to make sure it is updated and only use credible third party provider for our non in-house developed software; Applying standard, well reviewed, and reputable encryption; Giving training to our IT and software development team of our facility on the practice of secure coding; Applying the strengthening configuration to harden our database security.

Implementing PR-IP.3 "Configuration change control processes are in place" are done through processes that monitor system configuration such as operating system and software, and implement secure approaches such as access management and credential protection. Deriving fro CIS CSC 3, we nned to establish standard secure configurations of your operating systems and software applications, test all process that involves automation, implementing two factor authentication in a critical area of the system, and compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization.

Managing, documenting, and testing recovery plans are procedures that implement subcategories PR-IP.9 and PR-IP.10. By referencing from CIS CSC 19 and 20, the applications of this sub categories includes assigning jobs and responsibility to certain people who work in the operation including from the system management and cyber security team will help the recovery plan work seamlessly when an accident happens. These employees need to be always aware and trained, tested, and develop these plans since incidents can never be predicted. Testing the plan can include internal and external tests in a separated environment and the result can be used to measure the performance of our recovery team and to improve security policy and measures.

As our facility needs to grow and develop tandemly with the area that we serve, we need to expand our facilities technology. The improvement of the system increases complexity and

could potentially open new vulnerabilities. Penetration Tests results that we obtain from implementing PR.IP.10 combined with incidents that happened if any are used to implement PR.IP-7: Protection processes are improved. Referencing from ISO 27001 Annex 16.1.6: Learning from Information Security Incidents, after an incident happens, we need to document it and place it under review to prevent future incidents from occurring again.

Procedure for Maintenance (PR.MA) Category
Maintenance is an integral part to ensure optimal protection of our facility cybersecurity aspect. To comply with NIST CSF security framework, we need to have a controlled maintenance procedure, documentation, and log access information.

Implementation of subcategories PR.MA-1 and PR.MA-2 requires Maintenance, Remote Maintenance, and repair of organizational assets are performed and logged, with approved and controlled tools. Referencing from ISO 27001 Annex A.11.2.4 Maintenance needs to be carried out on equipment at appropriate frequencies to ensure that it remains effectively functional and to reduce the risk of failure. Log information about these maintenance needs to be documented clearly. The beginning development of our facility most likely will have on site maintenance rather than remote maintenance. When our facility develops or in unavoidable instances that requires remote maintenance, it is good to consider a remote maintenance plan.

Procedure for Protective Technology (PR.PT) Category
Protective Technology can improve our system protection as well as preventing exposing vulnerabilities. In order to keep our protection solution work optimally, these solutions need to be managed to ensure the security and resilience of systems and assets, consistent with related policies, procedure.

We are referencing to CIS CSC 8 to apply the implementation subcategories PR.PT-2: Removable media is protected and its use restricted according to policy and PR.PT-4: Communications and control networks are protected. According to CIS CSC 8 about application software security, we need to ensure that the software that we use are still supported by the third part vendors. In case of a plan to discontinue support, our team needs to work to test the integrity of the new version integration. It is more recommended for our facility to keep our software updated as newer versions should improve the software security than staying with an older version until the support is discontinued. An example that we can take is the operating system that we use in our facility. Although upgrading software might increase some budget, we should keep our system updated and test the applications compatibility. It is also recommended to apply hardening technology in our database.

Application of PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities; an example is the standard secure configuration in the operating system. Workers and employees should be given limited privilege to prevent them from vulnerability risks such as escalating privilege or installing malicious software into system integrity. Protection against attack from private LAN to our system should be implemented to prevent attackers from gaining access into our secure network area. Managing our system with a two factor authentication technology when interacting with network devices is a good application of protective technology.

Detect Function

This function mainly deals with identifying appropriate procedures and cause in the case of cyber-attack events. As the organization has a well organized detect function, it allows them to identify any cyber threats as soon as possible before it gets worse and minimize the risk. Since “Detect” is one of the functions in the core framework, there are three categories for “Detect” to achieve its outcome, those are “Anomalies and Events,” “Security Continuous Monitoring,” and “Detection Processes.” In order to achieve each of these categories, there are sub-categories under each category. The list below is showing the sub-categories for each category:

- Anomalies and Events
    - A procedure of network operations and data flows for users and systems is well planned and managed.
    - Detected events are studied to understand attack targets and methods.
    - Event data are gathered from many sources and sensors.
    - Impact from this event is understood.
    - Threat alert thresholds are created.

- Security Continuous Monitoring
    - The network is kept monitored to detect any cyber threat events.
    - The physical environment is kept monitored to detect any cyber threat events.
    - Personnel activity is kept monitored to detect any cyber threat events.
    - Malicious code is detected.
    - Unauthorized mobile code is detected.
    - External service provider activity is kept monitored to detect any cyber threat events.
    - Monitoring for unauthorized personnel, connections, devices, and software is performed.
    - Scanning for vulnerabilities are conducted.

- Detection Processes
    - Roles and responsibilities for detections are specified.
    - Activities conducted are meeting the requirements.
    - Detection processes are assessed.
    - Event detection information communication channel is effective .
    - Detection procedures are improving over the time.

Anomalies and Events

Anomalies and events have responsibilities of detecting and understanding the effect on the organization from that threat. In other words, organisations and their security teams must be

well understood, to be able to detect any kind of anomalous activities appropriately, otherwise, it may cause serious security threats to the organisation. I will pick up a few references that are necessary from ISO 27001 in order to meet this sub-category.

Procedure of Network Operations and Data Flows for Users and Systems

First sub-category under anomalies and events is, “A procedure of network operations and data flows for users and systems is well planned and managed.” In order to meet this criterion, according to ISO27001, “Detailed operating procedures must be documented and accessible by all users who are required.” By providing detailed operating procedures to each personnel, it makes sure everyone has the same standard of knowledge for effective operation of systems for new staff or changing resources. Moreover, it is very important in case of disaster to recover the system, business continuity. It is very crucial that documents are kept up to date, any changes are made in earlier periods and reviews are done periodically. Furthermore, since detect function has an important role to make sure if there are any intruders in the organisation, if so then people from detection function will be able to make appropriate action which allow them to make sure it is secure and minimise the risk.

Secondly, the second sub-category is, “Change management,” this is required where the organisation with handling of information and systems that affect information security need to be managed. It is essential to have strictly controlled change management in most of the areas in the organisation to make sure changes are suitable, effective, authorised and purpose for to minimise the risk for malicious or accidental compromise, it also includes updates to the systems as well. In order to make sure to keep track of change procedures are done correctly, audit logs are required. This is because the auditor will make advice on the change procedures that were made to make sure if it is appropriate and meeting the standard for the organisation. Since the system is changing, it is important that all employees know how to handle the system, otherwise there is a need for training as well as newly updated documented operating procedures.

Thirdly, the third sub-category is, “Network Controls,” many organisations have systems connected to its network, which plays the essential role, which requires a well managed and controlled network, in appropriate procedures to keep the information safe. The organisation must control the network according to its business requirements, risk assessment, classifications and division requirements that will satisfy. In order to make sure that the organisation has implemented effective and appropriate network controls, the auditor will be assessing what has been changed. Network controls allow the organisation to safeguard its network, for example by use of access control, detect function can monitor who and which devices are connected to the organisational network, if there is any suspicious device or personal, the function will be able to pass the information to respond function.

Fourthly, the fourth sub-category is, “Security of Network Services,” security systems, service levels and management requirements within the organisation must be identified and specified in the network service agreements. What this means is that the organisation must make sure that they document all the security measures they are taking to secure its

network service, whether the services are provided by internally or externally. In order to make sure that the organisation has implemented effective and appropriate network security that meets the business and security requirements, the auditor will be assessing the design of the network security structure by taking in account of a risk assessment. Risk assessment is a tool that can be done in a spreadsheet, ISMS.online, by specialist and expensive security risk assessment applications to identify, assess, and implement security to meet the business requirement. By documenting the security of network services, if in case of cyber-attack, detect function may be able to identify where the vulnerability is located within the organisation network and understand what the threat can cause further to the organisation resources.

Implementing procedures for data flow for users and systems within the water supply systems network, procedures for enforcement which the data flow will be compared against the security policy as well as the source and destination of the data flow. In the case, procedures for blocking certain data flow and alerting systems must be in place, such as use of firewalls, in order to prevent external data flow that is not allowed. Use of firewalls and monitoring of inbound and outbound data flow monitors are inplace to monitor if there are any unusual traffic patterns or suspicious data flow is not ongoing between internal water supply systems and external, and vice versa. System that prevents information already encrypted from bypassing content checking functions, in that case decrypt the information and block the data flow to make sure if the content does not harm any water supply systems. In the situation where automated checking is not possible, human interaction will be required to make sure of if there are any cybersecurity threats during the data flow. Network operating needs to be restricted carefully when employees connecting to a public network, which they are required to connect to organisation VPN in order to work from outside their business to make sure of there is a secure data flow communication. Monitoring of the information systems to detect unauthorized local, network, and remote connection, implemented through automated mechanisms to enable real-time monitoring. Allowing for if there are anyone who is attempting or connected to the water supply systems infrastructure network in anyways. Alerts will be sent to detection functions for early detection to minimise the impacts. At the water supply systems facility, use of intrusion detection systems for wireless networks to identify unauthorised devices and abnormal traffic patterns, not just limited to LAN connections but also for wireless access as well, due to employees carrying their smartphone and laptop with them which are connected to the wireless access points. .

Event Data are Gathered from many Sources and Sensors

Second subcategory under anomalies and events is, “Event data are gathered from many sources and sensors.” According to ISO27001, in order to meet this criterion “A.12.4.1 Event Logging” needs to be referred. Collecting event logs, for example, user activities, exceptions, faults and information security events allows the organisation to detect when the attack was initiated, the actual time. It must be produced, stored and evaluated on a regular basis, therefore, the organisation will be able to detect if there are any vulnerabilities that will likely to cause any threats in the future, for example weaknesses within the organisational networks, which can be fixed. Moreover, keeping logs of every activity including personal to systems, it allows for organisation to have strict security management, which leads to a

strategy for detecting anomalies as soon as possible and investigating threats. This enables safeguarding the organisational IT assets.

In the procedure for event data gathering from many sources and sensors at the water supply systems integration of automated audit review, analysis, and reporting mechanism can be placed, which allows continuous monitoring and identifying any anomalies. Through the reviews of event data gathered, analysis can be done by comparing the data that was collected over the times to see the trends and identification of cyber threats can be found earlier, no need to run vulnerability scanning over the time as well, which will be time consuming as well. In the case of cybersecurity incidents identified through collection of event data from sources and sensors, procedures of dynamic reconfiguration of IT assets must be in place for the incident handling. Examples such as changes to rules with network components, routers, access control lists, introduction system, firewalls and gateways. The procedures are in place to stop further attacks and safeguard the IT assets. Event data can be monitored through automated mechanisms and trigger any suspicious and anomaly events.

Moreover, throughout the collection of event data, once the suspicious and anomaly events are detected there must be a response plan. Water supply systems is required to produce an incident response plan:

- Plans ahead for implementing their incident response capability
- Meets the purpose, requirements for the water supply systems
- Identifying acceptable risks and cybersecurity threats that must be reported
- Identifying the levels of cybersecurity incidents to the water supply systems
- Identifying the resources and management support required for the incident handling

Impact from this Event is Understood & Threat Alert Thresholds are Created

Since “Impact from this Event is Understood” and “Threat Alert Thresholds are Created” have the same reference to ISO27001, which is “A.16.1.4 Assessment of & Decision on Information Security Events.” In case of any kind of anomaly event, before it is identified as a security breach, the incident must be first understood for decision making of what needs to be done to minimise the impact. Since from the monitoring and logging of the system, it might trigger as a threat, however no level of warning may be shown. Before taking an action, detect function has responsibility to understand the cause and level of this threat and decide the best way to minimise the further impact on organisation as well as on the clients. The focus for the minimising the impact is mainly on the availability for the service, integrity to make sure data is not amended and confidentiality to make sure no information is breached. Since by understanding the threat first, the detect function will be able to identify where the vulnerability is located and how it managed to get inside the system. By identifying these problems detect function can pass on the information to the respond function to minimise the risk in an appropriate and effective way.

In order for the impact of the event to be understood, the water supply system must undergo risk assessment, which measures the threats vulnerabilities, possibility and the impact on the infrastructure through various cybersecurity threats. It also needs to be considered that risk from external parties, such as the software companies and contractors where the water supply systems work along with. The documented risk assessment result must be produced and reviewed on a regular basis. During the reviewing of the risk assessment document, updates must be made if there are any changes to the IT systems, new threats and vulnerabilities are identified and distributed to the employees. Which allows all the employees to be aware and understand what procedures must be taken by them. Contingency plan must be in place, in case of during the period where an important objective is happening, contingency plan may be used depending on how severe the cybersecurity threat is on the water supply system infrastructure. Through contingency planning, IT assets that are critical may be taken further safeguards and countermeasures if a new threat to the water supply systems is detected. Which enables availability of water supply to the 200,000 inhabitants in the town. Water supply systems must create levels of cybersecurity incidents, which defines the procedures that must be taken according to how severe the event is, which also includes the acceptable risks for the organisations as well. This document must be protected from unauthorized personnels to protect from being shared and for the integrity of its document.

For example, at a water supply company, in case of threat, rather than trying to stop the threat on organisation, it is effective to first of all to understand the cause and level of the threat. According to the understanding of the threat, the organisation can decide what action to take depending on the priority on out of three of availability, integrity or confidentiality, to minimise the further risks. Moreover, by understanding the threat level and impact on organisation first, they will be able to take action accordingly and effectively, this will lead to good communication between employees at different levels of hierarchy, as a result can deal with the threat efficiently with less impact on organisation and 20,000 inhabitants. Furthermore, in future if there are similar threats on the organisation, since detect function has experience from the past, they have better understanding and high procedures to handle, which enables them to deal with it much quicker.

Security Continuous Monitoring

The responsibility for this category is that the organisation has in place of monitoring systems for their hardwares and softwares. By placing monitoring systems, it allows the organisation to detect anomalies and events quicker and make their decisions for the action to take. I will pick up references that are necessary from ISO 27001 in order to meet this sub-category for the water supply system.

The Physical Environment is Kept Monitored to Detect Any Cyber Threat Events

One of the subcategories in order to meet the criteria of Security Continuous Monitoring is, “The physical environment is kept monitored to detect any cyber threat events.” In order to meet this criteria, reference used according to ISO27001 is A.12.4.3 Administrator & Operator Logs.” This is to maintain the business system, keep monitored, logs to be protected and reviewed every certain period of time. Since people in the IT department have different roles, therefore, the water supply company must make sure that system administrators and operators have privilege to access logs. Other than system administrators and operators have no privilege to access logs except from who are required. Since logs play the essential roles for the water supply system as it keeps record of all the events, in the scenario of cyber threat the detect function will be able to detect where the vulnerability is within the system.

In order to have access to the water supply systems facility, at the entrance there must be a checkpoint allocated to verify individuals who are accessing, everyone from employees to visitors. With visitors, security and one of the employees must escort around the facility to make sure to monitor their activities and keep the systems safe from any suspicious activities during the system maintenance. Even to the special room such as server rooms for the water supply database, backup and storage room, network room, etc, there must be a checkpoint to make sure if these people are all authorized. For the checkpoints and inspection of the facility, there must be security 24/7 in order to make sure to keep the environment safe from unauthorized access to the facility. Combination locks, drawers with locks and keys must be locked and kept at the safe place to make sure of keeping information safe, inaccessible to the room and documents by unauthorised persons. Physical access logs, at what time, by which person was entered to which room and what was done, this record must be made and reviewed over the time. This enables the water supply organisation to keep track of in case of cybersecurity threat to the systems, it is one of the resources and evidence to identify physical activity and one way to reduce the threat. Furthermore, installation of intrusion alarms and surveillance equipment such as CCTVs, which must be installed in every room in the facility and entrance to the facility. Installation of automated recognition of employees through such as fingerprint scanner, face detection through CCTVs, voice match and many more to monitor the environment to make sure if it is only accessed by the authorised personnels.

Which all these measures allow to safeguard the water supply systems from physical cyber attacks, since threats can come from any vectors, over network, physically or installation of virus into the systems and many more.

Personnel Activity is Kept Monitored to Detect Any Cyber Threat Events

Second subcategory is “Personnel activity is kept monitored to detect any cyber threat events,” reference from ISO27001 to be used is “A.12.2.1 Controls Against Malware.”

Personal activity is monitored alongside protecting the system against malware, which is implemented together. In order to keep protected against malware there many approaches apart from anti-virus software, must be taken into the account, since only anti-virus software is not the best solution. Companies must consider personal restrictions such as use of external media, e.g. USB drives to prevent from any kind activities such as downloading software or taking business data. Secondly, user access controls such as restrictions on downloading software by employees, since this could be a virus. Making sure all the computers are up to date, since the old update may consist of vulnerabilities which lead to a cyber threat, as well as the anti-virus software are also kept up to date and have latest signatures.

In order to make sure to keep monitoring of personnel activities, user account privilege must be set by the IT department. Setting of authorized users depending on which department where they work, have access to the specific data, information and different privileges, must be in place and considered carefully. As it may lead to a risk to the systems by a non-authorized department in the water supply systems access systems to the water management, causing the systems to fail or lead to cybersecurity threats. Monitoring of computer usage must be carefully monitored, for example, anomaly activities of the system, such as accessing water supply systems from different places on the same day. Which is part of the detection process of identifying the sign of a threat for the water supply systems of being under attack. Moreover, IT department who are responsible for detection have the ability to disable accounts who are causing a threat or risk to the water supply systems by using the advantage of privilege of its user account. This measure must be taken to make sure if it does not cause any damage to the water supply systems. In order to secure the unused accounts, the water supply system implements features that will automatically disable the account after a certain period of time. This allows there is no unauthorized access to the systems and mitigates the risks from harm by making use of privileges from this account. Monitoring for information disclosure must be monitored as well, for example vulnerabilities, information, code that's been used in software at the water supply systems being uploaded on the Internet, which are threats for the organisation. In order to keep monitor of these activities, use of automated tools to identify if the information has been publicized. Software usage restrictions must be in place for example to make sure that employees are not making use of softwares for other purposes which there must be a policy as well for the use of it. For example, the information of the water supply system is not shared to the unauthorized personnels. Moreover, use of open source software is not used within the water supply systems due to the ability to amend the code freely, which employees may change the source code to make vulnerabilities, viruses or threats to the systems. Which will cause a huge cybersecurity threat to the systems. Furthermore, there must be software installation policy, which documents the software allowed to install, the right use of installing software, and consequences to the employee for installing prohibited software. Installation of software which is approved to be installed by water supply, and updates and security patches for downloading software is permitted. However, prohibited actions such as installing non-approved softwares and software that causes harm to the water supply systems. Furthermore, installation of privilege and alert system for software installation can be implemented to the organisational group policy. Which enables only the user with higher privilege such as administrator can install software or who are required to do maintenance. Otherwise, alert the user and keep the logging of the activities.

External service provider activity is kept monitored to detect any cyber threat events & Monitoring for unauthorized personnel, connections, devices, and software is performed

Thirdly, since “External service provider activity is kept monitored to detect any cyber threat events” and “Monitoring for unauthorized personnel, connections, devices and software is performed” have the same references therefore I am going to combine them together. The first reference from ISO27001 is “A.14.2.7 Outsourced Development.” In order to meet these two subcategories, the water supply company must have clear policy for outsourced development, what this means is that since the water supply company may use softwares from other companies, therefore they have to specify the requirements for the security under the agreement and must monitor and assist the activity of system development. Otherwise, if the development is not assisted or monitored by the water company, the security requirement to meet the policy made by them will not be satisfied. Furthermore, people from outside the organisation, there must be a policy that these people must undergo training such as security awareness training and awareness programmes and communications.

In order to keep monitoring of external service providers and unauthorized personnel, connections devices, and software, continuous monitoring must be kept in place at the water supply system and assessment for the security procedure at the external service provider must be conducted by the water supply system. In order to monitor external service providers’ activities, the water supply system may send assessment teams from the organisation to make sure of if there are any threats that may affect the water supply systems. During the monitor for unauthorized personnel, connections, devices, and software, at water supply systems they may employ automated scanning systems and results may be compared against the one collected from other periods of time. This enables for trend analysis to detect anomaly activities and events. During the external service provider activity monitoring, the water supply systems may check for changes that were made in the configurations, this includes types of changes that were made to their systems, reviewing of those changes if it is appropriate and documenting those changes for as a record. Even to monitor for unauthorized activities within the water supply systems/in the organisation, the organisation may employ a feature for automatic scanning, this produces a document for any configuration changes in the systems, determines if the configuration was accepted or not, and notify the changes to the personnels at the detect functions. During the maintenance at water supply systems, there may be some hardware being connected to the systems or employees may bring their own device (BYOT), the automated detect mechanism may identify if the devices are authorized and acceptable or the configuration to the systems made during the maintenance is acceptable according to the baseline. This enables to minimise the further impact to the water supply systems infrastructure due to the early detection or threats. In the case of when unauthorized components are detected, procedures are in place, automatic detection feature triggers and automates the process to move that unauthorized devices and connection made to another area of the network. Central repository for the inventory of information systems is in place, which enables it to effectively identify if the hardware, software and firmware assets are authorized, the location of where it is located, and if it is not compromised and vulnerable from cybersecurity threats. Central

repositories have everything in one place which enables to minimise the time for locating where an individual information system is located.

Scanning for vulnerabilities are conducted

Lastly, in order to meet the requirement for “Scanning for vulnerabilities are conducted,” reference from ISO27001 “A.12.6.1 Management of Technical Vulnerabilities” must be met. In case of cyber threat, the detect function must understand and find out the vulnerabilities of the system as soon as possible in order to what action to take in order to minimise the damage to the organisation. There must be a policy for procedures to take in case of a threat, step by step to scan the water management systems in order to minimise the damage and to make sure continued availability and integrity of the systems. Having the policy for the processes of scanning for vulnerabilities in the event of threat, clear procedures allow for effective understanding and detecting vulnerabilities in the systems. Moreover, will be able to efficiently resolve the problems, since the auditors are expecting to see there is a policy which documents the procedures for it. Furthermore, over time, there must be constant scanning for vulnerabilities. Example components that are required to be scanned are computers, routers, application systems for the management of the water components. Which, one of the hardwares such as computers may have been infected at some point, in order to safeguard from these kinds of scenarios, there must be vulnerability scanning conducted on a regular basis to make sure if there are no threats or vulnerabilities to the systems. The analysis can be conducted in a number of ways:

- Web-based application scanning
- Static analysis
- Binary analysers
- Code reviews - May not be ideal

Vulnerability scannings are such as:

- Scanning for path
- Accessibility to the functions, network ports, protocols and services (Access privileges)
- Scanning for the unacceptable or improper configuration wit in the system

Through the scanning, vulnerability scan is analysed, report and results are compared against the organisation security policy, furthermore to understand the impact on the water supply systems. The use of automated vulnerability scanning and results are compared between the one from the past to see any difference or anomaly in the results, allowing for identifying vulnerabilities to minimise the further effect.

At the water supply company since the systems are playing important roles in order to deliver water for 200,000 inhabitants in the town. Therefore, in order to minimise the effect on the clients of not being able to use water, there must be a well documented policy of what actions to take in case of the event. Therefore, by having it, the availability of water for the

clients will be continued and only a small amount of damage will be done to the system, since the vulnerabilities can be patched in a short period of time since the threat was triggered.

Detection Processes

Third category is detection processes, the purpose of having this in place is to make sure that detection processes and procedures are maintained and tested regularly to be able to handle any kind of unforeseen circumstances. As detection processes and procedures are organised, the impact on the water supply system can be reduced due to detection of vulnerabilities and threats before it gets worse and even mitigate it. I will pick up references that are necessary from ISO 27001 in order to meet this sub-category for the water supply system.

Roles and responsibilities for detections are specified

First subcategory is “Roles and responsibilities for detections are specified,” must be met. At the water supply system, there must be responsibilities assigned to every personnel of what they’re roles are for protecting information security. These responsibilities can be general, not in detail or specific, in much more detail. By in general such as, “Check for vulnerabilities” and as in specific such as, “Protect the water supply tank database.” However, in case of water supply systems, there are many systems functioning in the organisation, such as water pressure, water purity, level, and many more, therefore it is important to have specific responsibilities in place, thus people understand what they’re roles are and no confusion between personnels who is responsible for what. The delegation of responsibilities must be given to each function or department within the water supply systems, for example, first function where they check water level, second function tank level, third function water routing and so on. Moreover, the auditor will be making sure if the organisation has made a reasonable decision to allocate personnel and responsibilities to be able to safeguard water supply systems.

Secondly, all employees working in the water supply system must undergo awareness education and training in order to safeguard the organisation from any kinds of cyber incidents. Moreover, as mentioned in the first category, any changes to organisational policies and procedures, the employees must receive updates to those changes. At the water supply system, there are many changes that will happen due to software updates. Also awareness education and training must be done by all the employees at a regular period. Therefore, all the employees who are responsible for detection are prepared and know the appropriate procedures they will have to take, which can minimise and even mitigate the impact to the systems.

In order to delegate the roles and responsibilities:

- There are written incident plans for roles for every employee of their procedures

- Roles and responsibilities are assigned for every employee in every department and have documentation for different levels of cybersecurity incidents

Detection processes are assessed

There must be testing for the system security needs to be done during the development phase. Specific testing for the system security over the development phase must be conducted in the water supply system, which must be checked by an authority. Before the testing of security functionality, the outcomes must be documented and must satisfy the business requirements for security. The auditor will want to see evidence that at the water supply system there was security testing has been conducted.

- Security assessment plan must include the followings:
    - Security controls and control improvements
    - Determining security control effectiveness
    - Responsibilities must be allocated.
- Measure the security controls in the water supply system in order to understand whether the control is in place currently and meets the security requirements.
- In place of a security assessment report documenting the outcomes.
- In place of the results of the security control assessment to individuals.
- At the water supply system, there must be reviewing of testing, training, and monitoring plans for risk management and risk response actions must be assessed.

In order to assess, there must be assessment teams, they may conduct IT assets monitoring, threat assessments, malicious user testing and many more, such as security feature assessments. Which enables for the readiness for any unforeseen circumstances of cybersecurity threats to the water supply systems. Further assessment, the team may analyse the trend through security control implementation, continuous monitoring activities, type of monitoring used and assess if any modifications need to be made. Which enables the effective detection process to be achieved and make sure the detection process is appropriate for the water supply systems. Penetration testing is conducted where an independent penetratin agent or team performs on water supply systems. They may perform any kind of scenario for the water supply systems to assess the detection procedures are effective as part of the security control assessments.

Event detection information communication channel is effective

In the water supply system, there must be good reporting of information security events and incidents in an efficient way and quickly. Employees working in the water supply system must be sure to obey to report cyber incidents and must be covered during the awareness and training procedure. For effective communication, once the cyber incident is discovered, it must be reported urgently to the personnel who are in charge of security administrators and documented.

In order for the communication channel to be effective the automated mechanism is in place. Allowing whenever suspicious activities and anomaly events are detected through the monitoring of the water supply systems, it will inform the team with early detection to prevent further damages. Furthermore, since communication between employees must happen on top of an automated alerting system, in order to enable the communication between employees to be effective, there must be a system security assessment for assessing the

teams and assessment roles and responsibilities as a part to make sure if there is good and effective communication between employees.

Respond Function Report

The "Respond" function's main objective is to maintain and enforce the procedures that enable parties to "act in respect of a detected cybersecurity event," as defined in the NIST framework. This function expands the efforts of the CISOs and their teams in the identification, protection and detection of functions and includes both threat mitigation and other critical measures.

While each component of the framework is critical, the processes and activities carried out as part of the "Respond" function have the potential to make or break the outcome of a cybersecurity event. Timely detection of the threat is extremely beneficial, but making quick efforts to analyze the issue, contain the damage, and carry out response plans can mean the difference between a large scale breach and an unsuccessful intrusion on the part of attackers.

To respond appropriately to a threat, a few key processes must be planned and implemented ahead of time. As a result, the CISO can effectively direct efforts and security teams understand their roles and responsibilities in responding to anomalous network activity while protecting the organization's most critical informational assets and supporting systems.

The "Respond" function needs to follow subcategories and their main tasks as listed below, to achieve its functionality.

1. Response planning [RS.RP]

Once the threat has been identified as part of the Detect function, the Respond function begins by executing previously created response procedures. These response plans must be carried out in a timely manner, either during or after the cybersecurity event, depending on the timeliness of threat detection.

- Recovery plan is executed during or after an event.

2. Communications [RS.CO]

The CISO and his or her team will be heavily reliant on this category. Internal and external stakeholders – typically led by the CISO and IT administrators – coordinate response activities and, if necessary, may seek assistance from law enforcement. Individuals follow response plans and understand their roles within them during this process. The initial threat event and any other associated events are reported on, and this data is shared with stakeholders to ensure coordinated consistency in accordance with response plans. Furthermore, details about the event can be voluntarily shared with key stakeholders outside the company.

- Personnel know their roles and order of operations when a response is needed
- Incidents are reported consistent with established criteria
- Information is shared consistent with response plans
- Coordination with stakeholders occurs consistent with response plans
- Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

3. Analysis [RS.AN]

CISOs and their teams examine and investigate detection system notifications during this process to assess the impact of the event as well as the adequacy of the enterprise's response. This is also when forensics are carried out.

- Notifications from detection systems are investigated
- The impact of the incident is understood
- Forensics are performed
- Incidents are categorized consistent with response plans
- 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)

4. Mitigation [RS.MI]

This crucial aspect includes processes to contain the incident, help deter it from spreading, and mitigate the threat's potential damage. Furthermore, any new vulnerabilities that have not previously been identified are documented and included in the company's overall documentation practices.

- Incidents are contained
- Incidents are mitigated
- Newly identified vulnerabilities are mitigated or documented as accepted risks

5. Improvements [RS.IM]

CISOs and stakeholders finally explore the knowledge gained from the response to this threat and work towards integrating these findings into future strategies of response.

- Response plans incorporate lessons learned
- Response strategies are updated

Recovery plan is executed during or after an event

It is important to distinguish between an incident that puts personally identifiable information (later referred to in this report as PII) at risk and one for which the organization will use PII to assist in responding to the incident. An organization may need to take different steps in its response plan depending on such differences. For example, when PII is at risk, an organization may need to consider which security activities to perform, whereas when PII is used for response, an organization may need to consider how to minimize the use of PII to

protect an individual’s privacy or civil liberties. As water supply systems face a variety of threats, from corrupted data files to viruses to natural disasters. In the event of an incident, the susceptibility to certain threat events can be mitigated by means of relevant standard operating procedures. For example, frequent events such as erroneously deleting a file can usually be fixed by restoring the backup file. More severe threats like natural disaster outages are usually covered in the contingency plan of an organisation.
A virus, another malicious code or an intruding system (whether an insider or an outsider) can also cause threats.

They can refer more generally to incidents without a technical expert's answer that could result in serious damage. The organization experiencing a denial service attack would be an example of a threat event requiring immediate technical response. The incident response team's response team needs to act rapidly to reduce its impact on the organization in this kind of attack. The definition of a threat event is flexible and can vary depending on the organisation. The threats to systems and networks posed by hackers and malicious code are well-known, however, it is still unpredictable how harmful events occur.

In a water supply system, it would be the best decision to plan the recovery steps and execute them while considering possible severe damage in terms of physical and financial aspects. According to ISO/IEC 27001, a Disaster Recovery Plan (DRP) is required to follow the mentioned criterias listed in ISO/IEC 27031 where the organizations need to implement Business Continuity Management (BCM) precautions and ICT (Information and Communication Technology) Readiness for Business Continuity (IRBC), to be able to conform with highest standards of readiness for disaster recovery.

Personnel know their roles and order of operations when a response is needed
One employee should be responsible for the incident response, with one or more designated substitutes. This person monitors and evaluates the work of the outsourcer in a fully outsourced model. In general, all other models have a team manager and one or more representatives in the absence of a team manager. Managers perform a range of tasks, including liaising with top management and other teams and institutions, resolving crises and ensuring the staff, resources and skills required.

Water supply systems require types of incident response teams that are very skilled in terms of the capabilities of high mobility and making quick-correct responses. Therefore, especially the managers must be technically skilled and be able to communicate with a wide range of audiences in particular. Ultimately, managers are responsible for ensuring proper performance of incident response activities. Beside the team manager and assistant, a number of teams are also technically led by people with strong technical knowledge and experience in response to incidents who take over and ultimately take over the quality of the technical work of the team. The technical lead position should not be confused with the incident lead situation.

Larger teams often assign the main POC for handling a specific incident to an incident lead; the lead of the incident is held responsible for handling the incident. The incident management may not effectively process the incident, but instead coordinate the actions of the handler, collect information from the handlebars, provide incident updates to other groups and ensure that team needs are met, depending on the size of the incident response

team and on the size of the incident response team. Incident response team members should have excellent technical skills such as system management, network management, programming, technical support or intrusion detection.

Each team member should have good skills and critical thinking skills to solve problems. No team member must be a technical expert - this will be determined in a large measure by practical and financing considerations - but it is essential for each major technological field to have at least one highly skilled person (e.g. commonly attacking systems and applications). Some team members specializing in specific technical areas, for example network intrusion detection, malware analysis and forensics, may also be helpful. It is also often useful to bring technicians who normally do not belong to a team temporarily.

Incidents are reported consistent with established criteria and Information is shared consistent with response plans
According to NIST SP 800-53, structure of the organization and definition of roles, responsibilities and authority levels; should include confiscating or disconnecting equipment and monitoring suspect actions by the incident response team, reporting requirements for certain types of incidents and external communication, information sharing guidelines (e.g., sharing of information, etc.). The correct coordination and communication between members of the incident response teams could help reduce cumulative attacks and their powerful effect on the systems on a larger scale. Furthermore, the false implementations of the Response Plan should be notified either to the Manager or the person who takes care of the communications among team members.

Coordination with stakeholders occurs consistent with response plans
Stakeholders and other types of partner parties of an organization, especially for a water supply system, would need to be informed quickly and conforming to the standards mentioned in ISO/IEC 27001 and 29100. The authorization boundaries process has significant impacts on risk management and is therefore an organizational activity that needs coordination between key stakeholders. The process takes into account mission and business requirements, safety and privacy requirements and organizational costs.

The corporate architecture is a common language for discussing risks management issues relating to missions, business processes and the objectives of performance, enabling better coordination and integration of efforts and investments across organizational and business borders for more efficient and cost-effective use of IT across organizations.

Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
Especially in case of attacks against the mass population of water supply systems, which is highly possible due to their similar preferences of IT solutions, the organizations must communicate with external parties during incident handling, such as other incident response teams, law enforcement, the media, sellers and victims organizations. Since such communication often needs to be made quickly, organizations need to define guidelines on communication so that only the right parties are given adequate information.

Notifications from detection systems are investigated and The impact of the incident is understood

As part of the corporate risk management process, organizations benefit significantly from the conduct of risk assessments. Once the risk assessments have been completed, however, it is prudent for companies to invest some time to keep the evaluations up to date. Maintaining a risk assessment currency requires support from a risk monitoring step (e.g. observation of changings in operational IT systems and environments or analysis of risk awareness monitoring results). Keeping risk assessments current offers many potential benefits, including timely, relevant information that enables senior managers to conduct risk management in close real time. Following the suggestions of NIST SP 800-53 and CIS CSC 19, a water supply system would benefit greatly from well-conducted incident analysis both for the past and current incidents. Especially, understanding the severity of an incident would shape the nature of strength of a possible response.

Forensics are performed
The best response to attackers go through well-performed forensics practices to ensure every harmful action in terms of cybersecurity against a water supply system faces its punishments. According to NIST SP 800-86, the number of crimes involving computers has grown over the last ten years, driving an increase in firms and products to help law enforcement detect who, what, where and how crimes are based on computer evidence. Computer and forensics networks have evolved to ensure that computer crime evidence is presented correctly in court. Forensic instruments and techniques are usually used to investigate the event by investigating suspect systems, collecting and preserving evidence, reconstructing events and evaluating the current state of events in connection with criminal investigations and computer security event handling.

Consequently after the forensics have been performed, the incidents can be categorized according to the Response Plan, also using the outcomes from the forensics as reports, for clearer feedback of what could be needed for further improvement.

Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external source
Previously listed elements of the Response Plan make up the general inputs and outputs of this step. On a larger scale, water supply systems can affect each other under circumstances of being attacked, considering the possibilities of parts of their systems being connected to each other. Thus, supported by NIST SP 800-53, the network of their incident response teams and their implementations of the general response practices are important to give more information to each other for achieving better cooperation in that sense.

Incidents are contained and mitigated
According to ISO/IEC 27001, before an incident overwhelms or increases damage, containment is important. Most incidents require containment. Early during each incident, this is an important consideration. Containment gives time to develop a tailor-made remedial strategy. Decision making (e.g. shutting down, disconnecting it from a network, disabling certain functions) is an essential element in the containment. Such decisions can be made much easier if the incident is contained in default strategies and procedures. Organizations should identify and develop strategies for acceptable risks when dealing with incidents. The strategies for containment differ according to the type of incident. For example, email infection strategies are quite different from those of a network-based DDoS attack. Each of these could be very different approaches. For each major type of event, organizations

should create separate containment strategies with clearly documented criteria to facilitate decision-making.

Eliminating components of the incident, such as the deletion of malware and disability of broken user accounts, and the identification and elimination for any vulnerabilities that have been exploited, may be necessary after an incident has been contained. In order for the hosts affected to be remediated, it is important for them to be identified during their eradication. Eradication is either not required for some incidents or is carried out during the recovery process. When recovering, administrators return to normal operating systems, confirm that systems work normally and fix vulnerabilities to avoid similar incidents, if applicable.

Recovery may include such measures as clean backup restore systems, scratch reconstruction, replacement of compromised files with clean releases, installation of patches, password change and tightening of network security perimeter (e.g., firewall rulesets, boundary router access control lists). The recovery process often involves higher levels of system logging or network monitoring. Once a resource has been attacked successfully, it is often repeatedly attacked, or other resources within the organization are equally attacked.

Newly identified vulnerabilities are mitigated or documented as accepted risks
Following CIS CSC 19, in a phased approach eradication and rehabilitation should be carried out to prioritize remediation steps. The aim of the early phases should be to increase safety overall with relatively quick (daily to week) changes in value to prevent incidents of future importance. For major incidents, the recuperation can take months. The next phase should focus on longer-term changes and ongoing work to make the company as safe as possible, e.g. infrastructure changes.

Response plans incorporate lessons learned and Response strategies are updated
For further improvement of possible incident response practices in a water supply system, one of the most important elements of the incident response is the most frequently missed one: learning and improvement. In each event response team, new threats, improved technology and lessons learned should be reflected. Holding a "learnings" meeting with all parties involved after a major incident can be extremely helpful in improving safety measures and handling of an incident itself, optionally regularly following smaller occurrences as possible. In a single learning meeting, multiple incidents can be covered. This meeting offers an opportunity to conclude an incident by looking at what has happened, what has been done to interfere and how well an intervention has worked. Within several days of the end of the incident, the meeting should be held. (NIST SP 800-86, ISO/IEC 27001)

Recover Function

This function deals with recovering of systems in the organisation. In water supply systems, in case of cyber attack, they will have to recover the systems to make sure to be able to provide water to the town where there are 200,000 inhabitants. However, recover function does not only have the responsibility of recovering systems, but to recover the trust between

the customers as well. There are three categories for the water supply system to make sure to have in its NIST documentation.

- Recovery Planning
    - Execute recovery plan during or after a cybersecurity incident

- Improvements
    - Lessons are learned through the cybersecurity incident
    - Recovery strategies are improved

- Communications
    - Managing public relations
    - Repairing reputations
    - Communication between internal and external personnels for recovery

Recovery Planning

In recovery planning this is to make sure recovery processes and procedures are conducted and reviewed to make sure that the water supply systems are able to be restored after the cybersecurity incident.

Execute recovery plan during or after a cybersecurity incident
In the water supply system, there must be personnel assigned on what procedures they will have to conduct in case of a cybersecurity incident. The responsibles are:

- Collecting evidence immediately of the incident
- Conduct information security forensics analysis; the cause, what happened and what systems were involved and why it happened.
- If needed, increase of security awareness
- Check if all the systems are logged for later use
- Good communication between employees
- Managing fo security weaknesses

Recovery must be executed according to the business requirements and the priority. Also the water supply system must protect backup and restoration hardware, firmware, and software. Safeguarding of backup and restoration hardware, firmware and software allow the water supply system to be able to recover its assets and keep the availability. Which minimises the impact on 200,000 inhabitants in the town.
Also there can be in place of:

- Automated incident handling process for recovery of the infrastructure and the systems, without the need of human interactions
- Backups are conducted at a regular basis

Backup and restoration hardware, firmware and software must be protected for the use of recovery of the water supply systems.
Through backups the water supply systems must make sure that:

- All the IT system data in water supply systems must be made through automated backup on a regular basis.

- Complete backups are performed, such as the steps for imaging which allows for the fast recovery of the water supply systems infrastructure in the situation where systems go down through the cybersecurity threats.
- On a regular basis, the data of backup must be examined for data integrity, this is performed by conducting actual data restoration steps to make sure the backup is working as expected.
- Making sure for confidentiality of backups, protected through physical security by storing in the safe room where it is secured or by encrypting the disk. Applies when the backups are transferred over network, including cloud and remote backups.

Improvements

In the recovery process, while recovering water supply systems they must safeguard its infrastructure from future cybersecurity incidents. In order to achieve this water supply systems must incorporate lessons and improve its recovery strategies for future procedures.

Lessons are learned through the cybersecurity incident & Recovery strategies are improved

In the water supply system, after the cyber incident, the organisation must perform that they have gained knowledge from this threat by analysing and understanding security incidents. From this knowledge, it allows to reduce impact and minimise the risk of cyber threats in future. It is critical for employees in the water supply system to gain knowledge from the experience in order to keep water supply available for 200,000 inhabitants in the town.
In the case of a cybersecurity incident, this must be taken to the review and learning procedure. Once the review and learning stage have been completed, the policies may be updated and employees may undergo training.
Furthermore, for water supply systems to be improved over the time after the cybersecurity incident, they must conduct:

- Internal audits (Inside the organisation)
- Reviews from management (Top of the hierarchy of the function)
- External audits (Outside the organisation, cybersecurity researchers)
- Security incidents
- Security reviews and testing

Water supply systems may choose to share information with external organisations for the recovery of its infrastructure for the further security experts' knowledge and safeguard its assets at the same time while recovering.
There must be a contingency plan in place to recover from any unforeseen cybersecurity incidents.

- Have recovery objectives and restoration priorities
- Contingency roles, responsibilities are assigned to employees with contact information of those who is responsible for
- Maintaining of important missions and business functions
- Without causing of further impact on water supply system, conduct restoration of the infrastructure
- Distribution of contingency plan to the employees
- Coordination of contingency planning activities
- Improve and review contingency plan through the knowledge gained from previous cybersecurity incidents

- Addressing of changes in the contingency plan to the employees and testing must be conducted
- Protect the contingency plan from unauthorized personnels

In the contingency plan, there must be a procedure not just then for a cybersecurity incident, including disaster recovery plans, continuity of operations plans, crisis communication plans, etc.
Furthermore, the incident response plan must be reviewed to make sure all the strategies are effective and able to mitigate and minimise the risks from future cybersecurity threats. Once the updates to the incident response place are made, this must be shared with the employees in the water supply systems, and if there are any problems found during the implementation, execution or testing this must also be addressed. The changes may also be shared with the external personnels who are working along the water supply systems, such as internet providers, software companies and so on.

Communications

While recovering, effective communication must happen between internal and external of the business. Recovering the trust between the customers and water supply systems is required for the recovery of the reputation of the business. As well as external organisations such as cybersecurity experts which allows the water supply systems to be managed and recovered safely from further impact of the cybersecurity incidents. Allowing efficiently to recover the infrastructures and serve water to the 200,000 inhabitants in the town.

Managing public relations & Repairing reputations & Communication between internal and external personnels for recovery

In the water supply system, it is important to keep contacts with security specialists such as professional associations, which must be sustained. Furthermore, there must be a plan for communicating:

- What will be communicated with the party
- When will be communicated
- With who
- Who should lead the communication
- How is it done

Water supply system may share information with the security specialists to achieve more effective incident responses, which they may be able to provide with better resources to achieve and safeguard its system and restore it as soon as possible. However, only with the trusted and who's been working with the water supply system.
The contingency plans must be produced along external personnels in order to meet the contingency requirements. Which allows effective recovery of water supply systems due to clear procedures that have been already understood by the external personnels for the recovering process. Moreover, no conflicts between both parties where misunderstood by an external personnel can be reduced.
Restoring must be coordinated with the internal personnels as well, coordination of the systems must be done carefully to recover the infrastructure as soon as possible and effectively. In order to achieve this the water supply systems employees must coordinate the incident handling procedures, which distributes the roles and responsibilities effectively which enables the personnels from external will be able to understand what needs to be done by them to support the water supply systems infrastructure.

Framework Tiers

First of all, what is a framework tier?

These tiers play an important role in covering the wide range and variety of different security requirements and risk appetites of different organizations.

NIST CSF has an ability to adapt to organizations of different sizes, for example in a big corporate organization could already exist some cybersecurity measures and an existing team of cybersecurity specialists, therefore implementation of NIST CSF does not need to complete because some of it could already be taking place in such organization by the guidance of some other cybersecurity framework. On the other hand, small businesses do not have such a high risk appetite, small organizations have fewer channels of potential threats to come, therefore there is simply no need to implement NIST CSF from top to bottom.

In order to fit organizations of any size, NIST CSF has 4 different tiers to offer, each of which describes the degree to which an organization's cybersecurity risk management practices exhibit the characteristics described in the framework.

Those tiers also have their respective name, from the lowest tier to highest: Partial, Risk-informed, Repeatable, and lastly Adaptive.

About tiers properties.
Each tiers has 3 distinct properties:

- Risk Management Process:
    - This is about how an organization determines and understands its cybersecurity risks.
- Integrated Risk Management Program:
    - This is about what an organization does to resolve its risks.
- External Participation:
    - This is about how an organization understands its impact on others in its cybersecurity supply chain.

Tiers:

- Tier 1 – Partial:
    - An organization barely understands its risks and resolves them in an ad hoc manner.
    - And such an organization does not participate in resolving risks in its supply chain.
- Tier 2 – Risk-Informed:
    - An organization determines its risks but does not have a complete understanding of their impact.
    - Such an organization does implement necessary safeguards but poorly documented and not as often as it is preferable.

    - Has limited understanding of its impact on third parties.
- Tier 3 – Repeatable:
    - Risks are formally approved and are regularly updated.
    - Well established and documented procedures are taken to resolve risks.
    - Has complete understanding of its role and impact in its supply chain, and has all necessary contracts and policies in place.
- Tier 4 – Adaptive:
    - Risks understanding is based on all previous and current knowledge of risks. Any accident is being analyzed and gained knowledge is being documented and taken into consideration.
    - Has all policies formally approved on an organization-wide level. Any decisions are taking those policies into consideration. Cybersecurity is now a part of an organization.
    - An organization has complete understanding of its role and impact in its supply chain and ecosystem as whole and updates and related contracts and policies in real-time based on the circumstances.

Our thought process on deciding the tier of a water supply goes as follows:

A town with 20 000 inhabitants is considered as a big town that is on an edge of becoming a city, therefore it makes sense to set the tier for a water supply organization in the range of 2 or 3.

Water is an essential part of humans' everyday lives. Any disturbance in a water supply may cause a great impact on the whole town's life flow, at this point tier 2 is completely unacceptable and tier 3 is a go-to.

On the other hand, the amount of people within a certain locality does not grow fast, in rough numbers, a typical medium town grows by just a few percent over 10 or 20 years. Therefore the whole workflow of a water supply company is simple and pretty much static over many years. In other words, the water supply does not need to extend much, the hardware or software gets updated often, neither supply chain changes.

To conclude, it is undoubtedly that a water supply for a town of 20 000 inhabitants should use tier 3: The Repeatable tier.

Implementing a tier 3 for a water supply should not be hard to implement and maintain because its workflow is simple and pretty much static, which means that asset management and risk management do not have much to change.

Framework Profile

The table below is the Framework Profiles, which it positions the water supply system organisational requirements and objectives, acceptable risk for the organisation. Framework profile was produced based on Framework Core that we have identified that is most important to the water supply systems. Framework Profiles allows water supply systems to

enable them to make changes and improvements of their cybersecurity view by weighing their “Current” Profile and “Target” Profile. Since this water supply system is a big infrastructure as it is serving a town where there are 20,000 inhabitants, we made a research about the other water supply systems and based on the research, we have concluded our Framework Profile for this water supply systems. Framework Profile is produced voluntarily by the organisation, which means there is no answer for if the Profile is produced correctly or not. We made a research about other water supply systems and organisations where they are serving water to a big number of people. Based on the research and our Framework Core that we have documented, we produced this Framework Profile for our water supply systems. Therefore, this allows the water supply systems to identify what needs to be focused carefully to manage their cybersecurity point of view in order to safeguard from threats. Function column identifies the 5 functions from Framework Core, Identify, Protect, Detect, Respond and Recover, Category column identifies the category under the function, we have picked up the most important and relevant categories for every function. Subcategory column is the subcategory that lies under category and requirements/achievements need to be made in order to satisfy that category for the water supply system. Level column identifies how important the subcategory is important and an explanation about the regulation and importance of it. Budget is how costly it is to implement this subcategory and final last 2 columns Year 1 and Year 2 + identifies when this action needs to be taken. Year 1 identifies it needs to be created at the first year or as soon as possible and Year 2 + identifies it needs to be constantly reviewed.

Function	Category	Subcategory	Level	Budget	Year 1	Year 2 +
Identify	ID.AM	ID.AM-1	HIgh This should already be implemented by ISO 27001 as per A.8.1.1, all present within the organization devices and systems should be documented, their characteristics, their version or model as well as a unique identifier if present. MAC addresses for NICs on computers and other network units. For computer peripherals to document their VID and PID (vendor ID, product ID). All information should be updated according to all sorts of events, creation of the new device, processing, storage, transmission, deletion, or deconstruction.	$	X	
			Medium			
		ID.AM-2		$	X	X

			This should also have been implemented by A.8.1.1, where all software should be documented in very little detail. Starting with the name of the software/application, version, date, and location of download, as well as on what devices this software is installed. Any new software should also be added to the list. After removing some software, even if no devices use it, information about it should remain, in case we will need to install it back we will know exactly what version to install, or in case this software has damaged any devices we will be able to pass this software to a professional who will be able to provide a proper way to restore from that damage. Documenting assets does not require any expenses and does not take much time.			
		ID.AM-3	High Referred to as A.13.2.1, A.13.2.2, all the communication and data flow should be documented, from where to where the information goes, especially in places where information leaves the organization to third parties. As per ISO 27001, all this is already implemented and no other actions are required.	$	X	
		ID.AM-4	High Most often all cyber threats come from outside of the organization, therefore it is vital to document external information systems that this organization interacts with. ISO 27001 A.11.2.6 also documents all off-site equipment and assets, therefore external systems should be already cataloged and no other actions are required.	$	X	X
		ID.AM-5	Medium In addition to A.8.2.1 we should also document what resources of this organization are the most important to their business environment, in other words, which resources make the most money. It is also important to note	$	X	

			which resources are more critical and which are less, this way we will have a clear picture of what resources to prioritize our focus. Without this information, all the actions to reduce risk will be less cost-effective. Constructing such a document could take some time because it requires evaluation of all resources and their roles within the organization.			
		ID.AM-6	High With A.6.1.1 all information security responsibilities are already defined and allocated among parties. Besides that, from time-to-time, those roles and responsibilities must be rescaled because the supply chain changes gradually over time and it might require a complete re-evaluation of roles and responsibilities to ensure that they are distributed and established the most effective way possible. Implementing this control may require huge expenses depending on whether the existing workforce has the necessary skills and time for handling specific roles and responsibilities of cybersecurity, in the worst case this will require hiring specific professionals.	$$	X	
	ID.BE	ID.BE-1	Medium This subcategory is fully covered by ISO 27001 Annex 15. All the relationships and agreements are established. The organization has a complete understanding of its role in the supply chain and no changes are required.	$	X	X
		ID.BE-2	Medium This is a hard topic and can never be covered completely. It is well described by ISO 27001 Clause 4.1 but can always be extended and improved on the need.	$$	X	X
		ID.BE-3	Medium This subcategory ensures the organization focuses on its goal. It is not covered by ISO 27001, therefore, needs to be done from scratch. For a	$	X	X

			water supply organization, it is highly important that everyone has access to water and it is also important that there are no disturbances. But it is also vital that the quality of water is acceptable and pressure is good enough so that the water could get to most distant customers.Without a clear view of organizational objectives, it is impossible to appropriately calculate the risks associated with organizational activities. In our case, the most important objective is that all customers have constant access to water therefore anything that could cause disturbances in supplying water should be considered as a high priority.			
		ID.BE-4	Medium This subcategory is greatly covered by ISO 27001 A.11.2.2, A.11.2.3, A.12.1.3 and there is completely nothing that needs to be changed or added.	$	X	X
		ID.BE-5	High This category is well covered by ISO 27001 A.17.1 ensuring that service can continue its work under any condition, what is left to add is to define a normal state of work so that it will clear when something is not working correctly. In addition to A.17.2, it would be a good practice to test critical services from time-to-time.	$	X	
	ID.GV	ID.GV-1	High According to ISO 27001 A.5.1.1 policies are already established and communicated to employees and relevant external parties.	$	X	
		ID.GV-2	Medium This has been also covered and implemented by A.6.1.1 the same as ID.AM-6 and therefore no further actions are needed.	$$	X	X
		ID.GV-3	High This subcategory is in-depth described by a whole A.18 covering from the identification of applicable legislation and contractual requirements to the	$$	X	X

			regulation of cryptographic controls therefore there is nothing to change even if tier will be raised.			
		ID.GV-4	Medium Covered by ISO 27001 clause 6.	$	X	X
	ID.RA	ID.RA-1	High Covered by A.12.6.1, A.18.2.3 and no further actions are required.	$	X	
		ID.RA-2	Medium Besides reading news and forums regarding cyber threats I would recommend also stay informed regarding possible acts of terrorism, either civil or politic based, because a water supply company quite likely could become a target for such an event.	$	X	
		ID.RA-3	High Done according to ISO 27001 clause 6.1.2	$	X	
		ID.RA-4	Medium No actions required.	$	X	X
		ID.RA-5	Medium All the necessary information for determining risk is already being collected and no other changes here are required.	$	X	
		ID.RA-6	High An extended period of time without water could cause great damage therefore for a water supply it is highly vital to be able to resolve any kind of issues in the shortest time possible. This subcategory is already partly covered by ISO 27001 clause 6.1.3. But I would recommend identifying all the risk responses once again as well as carefully distributing risk responsibilities and priorities because this would help to avoid any disastrous consequences.	$	X	
	ID.RM	ID.RM-1	High In this category, all risk management processes must be accepted and controlled by stakeholders. All	$$	X	

			previously established practices should be always followed. For a water supply, whose work can be seen as simple and static at the first glance, it is hard not to forget to follow all policies and practices. Stakeholders should, from time to time, ensure that all policies are constantly followed and all employee's understanding of risks does not decay over time.			
		ID.RM-2	Medium Priority number one is properly prioritizing things. It is recommended that organizational risk tolerance is well determined and clearly expressed because it enables the organization to think saner during time crucial contingencies.	$	X	X
		ID.RM-3	 TODO			

Function	Category	Subcategory	Level	Budget	Year 1	Year 2 +
Protect	PR.AC	PR.AC-1	High Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. We need to keep the employee management and human resources in connection with our cybersecurity team to make sure that a certain person belongs to the correct department and given the right access, or revoked if they do not have the authority to access certain functionalities in the facility.	$	X	X
		PR.AC-2	High Physical limitation of access to most of the facility is crucial since we have to limit unauthorized access in the facility. There are many important functions in the facility where only authorized people in a particular department are allowed to access. Revoking the access is also important.	$	X	X
			Moderate			
		PR.AC-4		$	X	X

			A facility with employees that works in different departments incorporating the principles of least privilege and separation of duties will guarantee the probability of stolen identities to access crucial functionality in the system.			
		PR.AC-5	High Network integrity is protected, segregated, and segmented to limit unauthorized access to certain networks.	$$	X	
	PR.AT	PR.AT-1	Moderate Making sure all employees are informed and trained about cyber security practices in the company will limit social engineering attack that is often a problem caused by lack of knowledge from users who do not work directly in cyber security	$	x	x
		PR.AT-2	High Users with privileged access to certain facilities should be aware of the access they have and to know the higher responsibilities they have to not let unauthorized parties steal the access they have.	$	x	
		PR.AT-5	High Physical and cyber security personnel is one of the most important part in the protection function in which they are the last defender who should recognize any unauthorized access and should take action directly to forbid the access to certain functionalities	$	X	X
	PR.DS	PR.DS-1	High Guarantying the security of data that contains sensitive and detailed information about the way our water facility runs will enhance the security protection of the system. Such information could include information regarding chemicals that are used and the way it is regulated in our facility.	$	x	x
		PR.DS-4	Moderate			

			Adequate capacity to ensure availability is maintained and managed. Availability of access data such as log and information should be made accessible to manage problems such as troubleshooting	$		x
		PR.DS-8	High			
			In a system that relies heavily on hardware and software integration, integrity checking of hardware should be made as a priority to guarantee the data transfer is executed accordingly and resulted on the right action done by the hardware	$$	X	X
		PR.DS-6	High			
			Guaranteeing that software having the right integration with one another is important to keep the system runs. It is also good to make sure all updates of software and firmware are tested and verified when integrated to the current system.	$	x	x
		PR.DS-7	High			
			Separating development and testing environment is crucial in the water facility treatment to make sure that problems that might arise during the testing does not impact our service	$	x	x
	PR.IP					
		PR.IP-2				
			System development life cycle is implemented to always stay updated with the advancing technologies of cyber attack.	$		x
			Configuration change control processes are in place			
		PR.IP-5				
			The policies and regulations that are implemented into our physical system in the water facility should be met. Put in simple terms, the facility must establish secure areas that protect the valuable information and information assets only authorised people can access.	$	X	

			Recovery and response plans are implemented and managed to make sure our employees, cyber security team, and all the executive can act immediately to handle any security breach or other type of attacks			
		PR.IP-7				
			Protection processes are improved. In a city where the population would increase and additional requirements that need to be met when we improve our system also means that we need to improve our protection function to prevent unwanted vulnerabilities	$	X	X
		PR.IP-10				
			Response and recovery plans are tested to make sure recovery plan and all employees working on it understand the process	$	X	
		PR.IP-12				
			A vulnerability management plan is developed and implemented. In our system, the board management needs to proactively encourage the development of vulnerability tracing and management to start the process of prioritization of handling vulnerabilities with a strong and real KPI.			
	PR.MA	PR.MA-1	High			
			We need to correctly maintain all equipment to ensure the integrity of our system. The requirement for routine, preventative and reactive maintenance of equipment varies and should be carried out by the third-party who provides these equipment and to reduce the risk of failure in our system.	$$		X
	PR.PT	PR.PT-1	High			
			In a complicated system with tons of mechanical equipment that is controlled electronically, the behavior of the system, maintenance, and any interaction with the system must be collected as a log to help create better surveillance and also ease the process of troubleshooting.	$	X	X

		PR.PT-3	Moderate Limiting the functionality to only its essential capability making sure that any security breach or unauthorized access will not make the whole system down in our water facility.	$	X	
		PR.PT-4	High Communications and control networks are protected	$$	X	

Function	Category	Subcategory	Level	Budget	Year 1	Year 2 +
Detect	DE.AE	DE.AE-1	High Document for network operation and data flow must be established for all the employees. The document is up to date in order to detect any kind of anomaly events as soon as possible. The document must be kept up to date and reviewed.	$$	X	
		DE.AE-3	High Since water supply systems have many sensors, therefore it is important to gather many information from those in order to make sure if there are any suspicious or anomaly events. Furthermore, sensors are the most valuable source of information since they give many logs in real time. Moreover, this can be done automatically	$	X	
		DE.AE-4	Moderate The water supply system impact from the cyber threat must be understood well. Therefore, this allows the detection function to take action quickly once the threat is understood. Since this can be automated to analyse the impact, therefore the threat can be understood quickly.	$	X	
			High			
		DE.AE-5		$	X	

			At the water supply system it is crucial to create alert thresholds. This is in order to identify how high the level of cyber threat is on the organisation. Therefore, by creating one, it allows the detect function to understand what procedures they will have to take depending on different thresholds. Moreover, this can be identified automatically.			
	DE.CM	DE.CM-3	Moderate It is crucial to monitor personnel activities, since cyber incidents can occur from within the organisation. Therefore, water supply systems must be restricted such as use of USB ports, software so many more.	$	X	
		DE.CM-4	High Malicious code can be planted into systems from outside or inside the organization. It can be detected easily or maybe hidden which can cause huge damage to the water supply systems. Therefore, there must be constant monitoring for malicious code to be proceeded. Furthermore, it can be done with the use of softwares.	$	X	
		DE.CM-6 & DE.CM-7	Moderate It is important that the water supply company make sure that they work together with an external party where they provide softwares to make sure it meets the security requirements. Moreover, monitoring of suppliers. This will cost quite a lot and must be done in every few months' time interval.	$$	X	
		DE.CM-8	High Water supply systems must undergo vulnerability scans a few times a week or even a day. Since, vulnerabilities are the biggest threat for the water supply systems allowing hackers to take over the control, which will lead to big impact. Scans can be automatically using software.	$	X	
			High			
	DE.DP	DE.DP-1		$	X	

			There must be a delegation for who is responsible for what in the water supply systems. Therefore, in the case of a cyber incident the employees know who they need to contact, as well as they know what their responsibilities are. This allows productivity as well as minimise the impact.			
		DE.DP-3	High	$$	X	
			The detection procedure for the organisation must be tested to prepare for in any circumstances. This allows any cyber incident to be detected as soon as possible, as well as able to perform it smoothly without any problems handling the procedures. This must be performed regularly.			
		DE.DP-4	Moderate	$	X	
			In case of cyber incident, the information about this threat must be shared across the people within the organisation. It is important so that the water supply systems can be protected from further impact by the incident as employees know where they need to be protected and what further detection procedures must be taken.			

Function	Category	Subcategory	Level	Budget	Year 1	Year 2 +
Reponse	RS.RP	RS.RP-1	Moderate	$	X	
			Planning response against a possible incident would be crucial for industries that are more prone to attacks which could directly affect the industrial capabilities and the safety of the environment.			
	RS.CO	RS.CO-1	High	$	X	
			It is very important for the personnel to know their roles and order of operations when a response is needed, especially in any emergent situation for a water supply system to keep its function maintained correctly.			
		RS.CO-2	Moderate	$	X	

			At the water supply system, even though systematic error reporting of the personnel is important to keep the working environment disciplined, it is not crucial in terms of cyber security aspects for the betterment of the industrial capabilities of the water supply system.			
		RS.CO-3	High Sharing the information about possible events throughout the management of a water supply system would keep the workflow in a healthier condition and therefore causing a safer water supply system, and especially keeping it aligned with a response strategy would support the formation and continuation for a more secure water supply system.	$	X	
		RS.CO-4	High Consistency with the response plans when coordinating with stakeholders carry a big importance in case of a water supply system due to a possibility of any occurance of irregularities with law and required measures to be taken.	$	X	
		RS.CO-5	High The incident response plan includes steps for escalating incidents to the executive response team, which determines the appropriate stakeholders and when to communicate details of the incident. Therefore, this is very important to keep the water supply system ready for any emergent incident.	$	X	
	RS.AN	RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4	High Notification awareness, the clarity of shared information, general analysis and forensics are both very important for a water supply system to continue functioning while there is a cyber security incident that could affect the efficiency or the functionality itself.	$$	X	
	RS.MI	RS.MI-1	Moderate Containing any cyber security incidents against a water supply	$	X	

			system could not be difficult to perform, including the fact that the attacks are generally targeted against the circuit boards of the systems that control the main functionalities of such a system. Basic filters or firewalls would be helpful in this case.			
		RS.MI-2	High Mitigation of any incident is very important in terms of the future usability of any water supply system. Since they are very difficult to build and maintain, the preservation of the current facilitation is very important.	$$	X	
		RS.MI-3	Moderate Documentation of such new incidents are important for further and better mitigation to keep the functionality of the facility in a more efficient way. Future incidents could be easily dodged thanks to these precautions information.	$	X	
	RS.IM	RS.IM-1	Low In case of a cyber security incident, a water supply system would not benefit as much from incorporating response plans for the lessons learned, since the attacks would not be significantly more advanced than each other.	$	X	
		RS.IM-2	High Updating the response strategies is very important due to the fact that they would cumulatively support the future actions to be taken against any different types of incidents.	$		X

Function	Category	Subcategory	Level	Budget	Year 1	Year 2
Recover	RC.RP	RC.RP-1	High There must be a recovery procedure for what needs to be done in order to maintain the availability. This can be done through by assigning the responsibility to people in the organisation as well as the procedures for retaining incident information.	$$	X	
	RC.IM	RC.RP-1 &	High	$	X	

		RC.RP-2	It is important that the organisation take incidents from the past as a lesson so that the organisation will be able to gain knowledge about what can be done as a measure for future incidents.			
	RC.CO	RC.CO-1, RC.CO-2 & RC.CO-3	Moderate For water supply, communication between external and internal personnel from the organisation is an important part of the recovery. Communication between security experts allows recovery of the system. Communication between customers allows recovery of the trust and reputations.	$$	X	

Conclusion

The Five Functions of NIST guidelines of cyber security incident management have been covered. Each of these categories and subcategories are explained in detail in terms of their importance, needs to meet certain standards, description of tasks and expected outcomes that could be related to management and maintenance of a water supply system, especially from cybersecurity perspectives.

Covered aspects of NIST CSF are:

1. Identify
    a. Asset Management
    b. Business Environment
    c. Governance
    d. Risk Management
    e. Risk Management Strategy
    f.
2. Protect
    a. Access Control
    b. Awareness and Training
    c. Data Security
    d. Information Protection Process and Procedures
    e. Maintenance
    f. Protective Technology
3. Detect
    a. Anomalies and Events
    b. Security Continuous Monitoring
    c. Detection Processes
4. Respond
    a. Response Planning
    b. Communications

    c. Analysis
    d. Mitigation
    e. Improvements
5. Recover
    a. Recovery Planning
    b. Improvements
    c. Communication

These points are based on well-known and established cybersecurity practices that are also supported by international standards. It perfectly covers all cybersecurity aspects and levels of required security. It is well thought and flexible enough to be valid in many cases of reflecting against a cyberthreat. NIST Framework for Cybersecurity is also important for correct risk management for a business, as well as water supply systems.

It is very important to understand the benefits of implementations of NIST framework and possible outcomes of those practices for several aspects such as cyberthreat containment, business continuity, healthy communication in between bodies and subsidiary bodies of an organization. Right now NIST CSF is voluntary to implement, while it is the responsibility of every individual and organization to understand the risks they are putting on themselves and their customers. Even a slight data breach can cause not just a huge fine but also permanently worsen reputation, and quite often facing strict limitations of operation.

Resources:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

https://resources.infosecinstitute.com/topic/nist-csf-core-functions-detect/

http://www.esdebe.com/perch/resources/iso-27001-annex-s-control-mapping.pdf

https://www.isms.online/iso-27001/annex-a-12-operations-security/

https://www.isms.online/iso-27001/annex-a-13-communications-security/

https://www.synopsys.com/glossary/what-is-security-risk-assessment.html

https://www.isms.online/iso-27001/information-security-risk-assessment/

https://www.isms.online/iso-27001/annex-a-16-information-security-incident-management/

https://www.isms.online/iso-27001/annex-a-11-physical-and-environmental-security/

https://www.isms.online/iso-27001/annex-a-14-system-acquisition-development-and-maintenance/

https://www.isms.online/iso-27001/annex-a-15-supplier-relationships/

https://www.isms.online/iso-27001/annex-a-6-organisation-information-security/

https://www.isms.online/iso-27001/annex-a-7-human-resource-security/

https://www.isms.online/iso-27001/annex-a-14-system-acquisition-development-and-maintenance/

https://cybernetsecurity.com/industry-papers/CIS-Controls%20Version-7-cc-FINAL.PDF

https://cybernetsecurity.com/industry-papers/CIS-Controls%20Version-7-cc-FINAL.PDF

https://www.nist.gov/cyberframework

https://www.nist.gov/document/2018-04-16frameworkv11core1xlsx

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjJiODmxJnwAhUthf0HHf7eBNkQFjABegQIAxAD&url=https%3A%2F%2Fcsrc.nist.gov%2FCSRC%2Fmedia%2FPublications%2Fsp%2F800-53%2Frev-4%2Ffinal%2Fdocuments%2Fsp800_53_r4_final_word_errata_01_22_2015.docx&usg=AOvVaw1TTrVYDTuSKLGq0UJR9mng