Final Project: Cybersecurity Framework

Course: CYBR10004 - Cyber Security Assessment & Testing

Student Name: Brendan Ancheta

Date: August 4, 2025

Index

1. Business Information

The name of my company is ‘Unlimited Games,’ abbreviated to UG. They are a video game development studio based in Canada that releases games of various genres, with a main focus on multiplayer games. Starting up several years ago originally with only one office and a few dozen employees, they now have multiple physical offices based in Canada, with a large percentage of their employees working between their nearest location and remotely from home, where they can access a virtual work environment through the company’s VPN. While their main operations are based in Canada, they release their games on online storefronts such as Steam and their own personal website, which make their games available to other countries. However, most of their consumer base is primarily within North America. Below is a list of departments within the company:

- Art and Design
- Development/Programming
- HR
- IT/Support
- Finance
- Production
- Marketing
- Quality Assurance (QA)

Since they do have players within other regions of the world, while they don’t have other on premise sites they do rent out servers from providers in order to allow said international players low latency availability of their games. Most of their other required servers and resources related to business operations are either hosted on premises or through well known cloud providers, which as mentioned before their employees can access from their personal machines through the company’s virtual environment and VPN connection. Across their offices there are currently hundreds of employees, and with continued success of the company they hope to expand their operations further and to more regions. They have prided themselves on the quality and efficiency of their game development. However, due to increase in scope, they have had to rush together their non-game development based departments implementation within the last few years, which has most likely led to some potential holes in their company infrastructure. Notably, their current IT/Security infrastructure is not quite up to date to appropriately handle their employee population size. While there has been a focus on development of networking and software requirements such as appropriate firewall and VPN setup, proper cyber security training across the company has yet to be widespread and standardized, especially as the company continues to hire more employees to keep with work demands. There are regular reports to IT of employees falling for phishing scams, though most of the impact of these attacks has primarily affected employees personally rather than a full company breach.

2. Risk Assessment

Step 1:
The company will not only hold data related to the business itself, but also customer data, such as login credentials to their accounts related to the game, and potentially payment information for when a customer runs a transaction through the company's website. Losing specifically company data of course could lead to heavy financial damages just like any other company through attack methods such as ransomware. However, if the source code of their games is leaked, this could very easily compromise their primary product, with the public being able to access and copy their games, or even find exploits with the code. This could lead to an increase in downtime on their games, as being multiplayer games they would rely on a constant uptime for their users to access their product, therefore affecting customer relations and sales. Should an increase in downtimes occur, it would be imperative to have proficient recovery methods in place to make sure their services are running as soon a possible. On top of this, if their database holding private customer information were leaked this would most likely result in both heavy legal costs and reputation damages.

Step 2:
Asset List:
Priorities given as low, medium, and high

- Company Data - High
  - Includes both important company records and employee personal data
  - As mentioned in step one, there is also the source code for the games included, meaning the company's product would also be at risk of damage should their database be compromised
- Consumer Data - High
  - If user credentials and transaction information of customers is not appropriately encrypted and secured, there can be huge repercussions both financially and reputationally
  - Very little tolerance for failure to secure said data
- Company On-Premises Machines - Medium
  - Presuming the offices are secure with proper industry standards, there should be low likelihood of physical theft
  - Concern lies in if there is potential for threat actors to gain physical unauthorized access to a machine while it remains in premises, i.e. are machines being left open and logged into when unattended
- Employee Personal Machines(Remote work) - Low to Medium
  - The likelihood of unauthorized access from a personal machine would depend from person to person, as well as the security configurations placed around the VPN
  - Without proper security training however, employees may become complacent when securing their own personal machines, causing them to be more susceptible phishing attacks, especially if they are targeted spear phishing attacks

- Company Work Servers (On-Premises) - High
    - If servers are compromised, an on-premise location could have all services to their employees inaccessible, of course impacting workflow and customer support
    - This would most likely be affected in tandem with the company's database as well, both of which could be targeted by ransomware as is common these days
    - The web server hosting the company's website would also most likely be included here, and being public access point if the site is not secure and has access to certain confidential data in the backend, this could leave it vulnerable to attacks such as code/SQL injection
- Game Servers (Rented) - Low
    - While servers being affected will cause downtime for players of the company's game, by renting servers from reputable providers they can offload maintenance and reputational to them in the cases cases of prolonged downtime

Step 3:
Notable Cyber Threats

- Natural Disasters/Unforeseen Events
    - While chances are low, it is good to have in place back up plans in the case of the unlikely possibility, as damages can be immense
- Phishing/Spear-Phishing
    - The company has hundreds of employees spread across Canada at differing locations, some even working from home
    - Different branches may make up their own standards on cyber security, and with a large employee base could make it more likely for more people to be susceptible to these attacks
- Physical Unauthorized access
    - While offices may be secure properly, without proper training it could prove a vulnerability with certain employee working remotely that may be leaving their work environment exposed
- Data Breaches/Loss
    - While this can take many forms and be catastrophic in their own ways, and industry specific example here would be a loss of source code and/or game assets that could severely impact game releases for the company
    - Depending on employee loyalty there could possibility for employees to leak data themselves either to the public or other game companies
- DDOS Attacks
    - Incredibly common within the game industry, being an easy way to disrupt online game uptime
    - Continuous attacks could with lackluster recovery from the company could affect reputation and overall sales

Step 4:

Potential Vulnerabilities:

- Non-Standardized Security Training
    - The company continues to expand its size, adding more to its employee base, making it harder to keep up with all of them to minimize the number of exploitable employees
    - Longtime employees can become the most susceptible to complacency due them becoming use to their daily work routines, and potentially overlooking common security threats
    - With multiple office locations it becomes more imperative to have a standardized up-to-date security protocols across the company, especially as the potential surface area for a cyber attack grows
- Zero-Day Vulnerabilities
    - With multiple offices working on different projects, it is unlikely for all of them to have the same resources, skill, and care given to their work
    - If there is a notable lack of quality assurance in a certain area, this could lead to potential exploits within their game releases and patches
    - In most cases these would probably be affecting the game infrastructure and balance, resulting in damage to the game/product quality
    - Worst case would be leaving vulnerability that could give threat actors access to confidential company data
- Data Miners
    - Common for games where users look into available information on a game to potentially find otherwise unreleased/confidential data
    - This can be as simple as analyzing patches to predict future content or looking into publicly available game files to find unrevealed assets
    - The damages of these activities are not always high, but due to legal ambiguity and dedicated communities toward it, it can be hard to fully protect against, especially if that information is important to upcoming product releases
- Remote Work in Public Areas
    - If there are employees opening their work environments from public places, such as a cafe or hotel, this could leave it open to unsecured networks or physical unauthorized access
    - To avoid a breach this way it would require proper set up of the company's VPN to make sure it is secure, and for employees to make sure they take care in not allowing for others to access their machines physically

Step 5:

Controls to Consider:

- Backups
    - Given that the company's main product is a digital service/entertainment, backups of data are not only important to business operations but also maintaining product integrity and quality
    - It can be assumed to be likely given the relevancy of this control that the company has taken measures to diversify and secure their backup system
- Security Training
    - As mentioned in Step 4, it is important for all employees to be alert and aware of potential security threats, and be trained properly in avoiding and dealing with them appropriately
    - Even though this company is heavily involved in the tech industry, employees will have a variety of skillsets, some being more technically experienced than others
    - On top of that, high technical experience and computer familiarity does not always mean one is aware of potential cyber threats
    - Considering just the quantity of employees, it is likely for there to be discrepancies in training and cyber security awareness across the company, especially as the company expands
- Penetration Testing
    - Being a game company, it makes sense most of their resources are dedicated to development of their games
    - This could lead to a lack of effort put into security measures are their digital interfaces, i.e. games, websites, virtual work environments, etc., as not all coders have a background or knowledge to properly secure their code against attackers
    - Dedicating more resources to properly testing programs before deploying them to the public could help mitigate zero-day vulnerabilities and exploits
- Least Privilege
    - Developers/Programmers often need certain access within a system to properly develop games and coding projects
    - That said, this can lead to them also having more access than needed, such as being allowed to both develop and deploy code at once
    - Separating roles and following principles of least privilege would mitigate potential damages if an employee account were compromised, as they would then have less data and services they could expose

Step 6:
Examining Risk Scenarios:

- Scenario 1: Game Exploit is Found
    - The severity and costs of this will vary depending on the effects of the exploit, i.e. only affects game infrastructure or directly accesses backend assets
    - If it only affects game infrastructure, costs would most be based on extra resources and work required needed to patch the issue, to restore the integrity of the product
    - If the exploit were to gain some form of backdoor access directly to company assets, it would have as severe impact as any other cyber attack intended to compromise a system
    - The first result is more likely, and can be common, as it can happen due to a simple bug in the game's code
    - Overall, general likelihood of occurrence is high, but severity and costs would have major fluctuation, with most worst case scenarios being unlikely
    - Given the company's main
- Scenario 2: Unauthorized Access by a Threat Actor
    - Due to weaknesses in security training, this could happen to exploitable employees through phishing attacks, leaving their computers exposed to the public, etc.
    - Depending on the access level of the affected employee, this could easily lead to ransomware and/or data leaks, leading to millions in damages
    - Impact would be even more severe if consumer data was also compromised through this breach
- Scenario 3: Website Comprised
    - This would be another way of breaching into company systems, only rather than targeting through social engineering or espionage based methods, the website is available to the public, so if there are vulnerabilities they can be very easy to discover and exploit
    - The website would most likely have some form of access to sensitive data, such as login credentials for users or company analytics
    - If measures aren't taken against malicious code/SQL injections and/or there are easy forms of backdoor access through the site, this would become a digital equivalent of not having a locked door to a physical office
    - Through SQL injections through query inputs on the site to data integrity being compromised, leading to malicious modifications or even deletions of data
    - If there wasn't a proper backup system in place this would make it incredibly difficult to accurately and quickly restore said data
- Scenario 4: DDOS Attacks Against Game Servers
    - This is of course a very common situation that could consistently affect the consumer base's access to the company's product

    - Granted, by ideally pushing game server upkeep to a reputable third-party vendor, they would hopefully have a secure system in place to efficiently defend and recover from said attacks
    - Costs related to it would also only be up to the renting costs for the servers, since as said ideally the server upkeep would be up to the vendor

Step 7:
Categorizing and Prioritizing Scenarios:

- Scoring Likelihood and Impact from 1-10
- Prioritizations by Scoring Total
    - Multiplying Likelihood and Impact for total
    - 1-25: Low
    - 26-50: Medium
    - 51-75: High
    - 76-100: Critical

- Scenario 1:
    - Likelihood - 6
    - Impact - 7*
        - Impact is situational so could be seen as lower or high, potentially being immense, but overall will concur notable costs and resources to resolve regardless, Potentially even reputational damage
    - Total: 42 - Medium
- Scenario 2:
    - Likelihood - 7
    - Impact - 10
    - Total: 70 - High
- Scenario 3:
    - Likelihood - 5
    - Impact - 8
    - Total: 40 - Medium
- Scenario 4:
    - Likelihood - 10
    - Impact - 2
    - Total: 20 - Low

Step 8:

This report encompasses the required documentation

3. COBIT

Capability will be measured on how prepared the company is for preventing and handling the defined risks. The importance and likelihood of the risks will also be considered in the goal capability level for each scenario.

- Risk Scenario 1: Game Exploit is Found
  - Capability Level - 4
    - With the company's focus on their development team being prominent, said staff have had experience dealing with major bugs in their games and more importantly how to properly remedy them in a timely manner.
  - Goal Level - 5
    - Even if the team is proficient at handling exploits found in their games, there is always room for improvement,
    - This could include analyzing these bugs and exploits and rather them simply fixing them, they can use what they player reaction and interaction with them as ways to improve further mechanisms, provided this is the most likely situation of affecting game infrastructure and not a critical breach into company systems through their games
    - Further investment into QA testing could also aid in ensuring projects are properly reviewed for vulnerabilities, potentially even involving the IT team to specifically check for security vulnerabilities
- Risk Scenario 2: Unauthorized Access by a Threat Actor
  - Capability Level - 2
    - General security measures have been implemented into the company, primarily within the backend networking and virtual environments
    - However, much of the issue still lies within human error, as many in the company are still exploitable and unaware of common social engineering attacks
  - Goal Level - 5 (at least 3)
    - Ideally the goal would be to reach a 5, however even reaching a 3 would indicate a greater effort has been put in placing in proper security training company-wide
    - If the company lacks the knowledge and/or resources to do so, they could inquire into third parties to aid in setting up proper security procedures
    - Overall, further teaching and enforcing awareness around cyber threats would help to remedy the current situation
- Risk Scenario 3: Website Comprised
  - Capability Level - 3
    - Given the capabilities of their programmers and designers, creating a functional and well performing website can be expected

        - Granted, even if a website is well put together and works well, does not inherently indicate it is free of vulnerabilities, even if it is unlikely
    - Goal Level - 4
        - Making sure the company's programmers are up-to-date on industry-standard secure coding practices will help ensure there are not leaving obvious flaws in their work
        - For example programming IDEs often have tools and commands that can be implemented into projects to help detect and block code injection attempts, so even being aware of this can be beneficial
- Risk Scenario 4: DDOS Attacks Against Game Servers
    - Capability Level - 3
        - Since servers are ideally managed by a vendor, they would hopefully be able to handle potential DDOSing to their servers, which would relieve resources from the company
        - One issue could be however, while the company does not have to handle game server issues, it also means when issues do arise it is out of their hands
        - This means if issues persist then the only available option is to rent further servers or move vendors
    - Goal Level - 5
        - As the company continues to expand and they gain more popularity with their games, there may come a time where renting their game servers may not be feasible
        - If the playerbase becomes too large, or there are specific server functionalities they would like control over, it may be a possible consideration to change to a different renting option that provides more personal upkeep and control, or even investing the resources to setup long-term servers themselves

4. CIS

Chosen Controls:

- Cis Control 4: Controlled Use of Administrative Privileges
  - This control would help with preventing basic breach attempts into company systems and employee accounts by controlling access permissions and practicing more effective account security
  - Sub Control 4.4: Use Unique Passwords
    - Simply enforcing better password usage company-wide can make most basic password breaches such as brute-forcing significantly less effective
    - Implementing requirements for special characters, making passwords longer, or using passphrases are some low-tech examples of how this control can be used
    - Keeping track of the number of employees who have their account breached through their passwords being guessed can help to measure this control
  - Sub Control 4.7: Limit Access to Scripting Tools
    - Being a game development company, there are likely to be many machines holding company scripting software
    - By ensuring said software is only used by certain users whose role directly pertains to requiring that software, should an account be breached it can make it less likely for that account to cause as significant damage
    - This includes in situations of a game exploit providing access to a company in-game account, or should an employee have their work account breached through phishing attempts, physical access, etc.
    - It would be important to keep track of what accounts have access to certain tools, as well as monitor if these accounts have reports of suspicious activity or if the employee attached to them have a history of being compromised
  - Sub Control 4.9: Log and Alert on Unsuccessful Administrative Account Login
    - Considering most attackers will want to aim for employees with administrative privileges the most, keeping track of failed login attempts to those accounts can potentially provide an early sign of a breach in progress
    - Most of the outlined risks could in worst case scenarios lead to admin account breaches, so this control can be used to help detect said risks before they have a chance to cause major damage
    - By recording what accounts are experiencing consistent unsuccessful logins, they can also be analyzed for patterns to help discover potentially vulnerable accounts

        - This can also indirectly show the effectiveness of control 4.4, as many failed logins on the same account could also indicate a strong password that was simply forgotten by the user

- Control 10: Data Recovery Capabilities
    - While mentioned before it can be expected for the company to have a proper backup system in place, due to the inexperience of the IT staff it could also be expected that said backups may not be properly tested or performed at points when and where they should be
    - Much of these risks can involve service disruption and/or data loss, and ensuring proper measures are taken in regards to recovery is essential for dealing with these issues
    - Sub Control 10.1: Ensure Regular Automated Backups
        - By setting up an automated system to run backups, this helps keep a regular schedule for when backups are run, ideally daily, while also minimizing the room for human error in the process, provided the system is set up correctly
        - The more up-to-date a backup is, the more effective it is in the case of an incident requiring them, such as rerolling a patch due to a game exploit, or if an attacker has compromised to company systems and wiped the databases through a breach
        - Logging when backups are run and if they ran successfully is vital for knowing if the automated system is working properly
    - Sub Control 10.3: Test Data on Backup Media
        - Backups are meaningless if they can't backup a system
        - Tests should be run regularly after a backup is created by running them through a simulated system recovery, which given the above automation more time can be spent on testing if backup creation is automatically handled
        - If there is a record of consistent failed recovery attempts, then this can be an indicator of an issue with the backup method in place
    - Sub Control 10.4: Protect Backups
        - Even if the company has considerable amount of backups with diverse storing methods, if the company is prone to certain breaches, as stated with the potential for employee accounts being compromised, then this can potential expose these backups just as much as the actual database if they are not under enhanced security
        - If backups are stored digitally they need the most modern encryption methods around them, and offline backups should held and stored by trusted company personnel or even reputable third party security

        - This can be measured simply on whether there are any backups that are able to be compromised during a breach, ideally through proper pen-testing run by the company, rather than an actual cyber attack

- Control 17: Implement a Security Awareness and Training Program
    - As stated before, one of the biggest weakness in the company is a growing lack of security awareness amongst the employees
    - Evidently, to help remedy this a proper security program should be implemented company-wide, and said program should regularly be updated and reissued amongst employees
    - Sub Control 17.1: Perform a Skills Gap Analysis
        - Before any training program should be put in place, there should be an evaluation of employees to determine what are the primary weakness regarding cyber security within company personnel
        - With this knowledge the presiding training can be more targeted on specific topics to focus remedying those are vulnerabilities first
        - This can be tracked by analyzing employees with a history of being breached and taking note on what mistakes they were usually making leading up to said breach
    - Sub Control 17.2: Deliver Training to Fill the Skill Gaps
        - By following best practices and looking into the areas of weakness within employees, a suitable training program can be put in place and standardized across the company
        - With better cyber security practices and awareness of threats becoming commonplace amongst employees, this should help to prevent a majority of common cyber attacks, and will set better precedent for future employees
        - There should be logs available in some form as to who has and has not undergone training, as well as metrics based on cyber security breaches before and after training
    - Sub Control 17.4: Update Awareness Content Frequently
        - Training must be continuously done by staff, with updates and improvements to the regimen every time it is deployed
        - Cyber Threats are always evolving, so there must always be attention to further improvements regarding the defense against them
        - On top of that, without consistent and regular training, it is easy for long term staff to become complacent if not kept up to date on cyber awareness
        - Metrics should be tracked on the quantity of breaches and number of breaches between each of the different training regimens to look for trends and patterns

- Control 18: Application Software Security
    - This control helps ensure programming staff stay aware of the various security measures they should be taking when developing and/or deploying code
    - This would help mitigate vulnerabilities within the company's games and web applications they release
    - Sub Control 18.1: Establish Secure Coding Practices
        - While coders may be proficient at creating well performing software, that does not always equate to knowing how to properly keep said software secure from vulnerabilities
        - There should always be an emphasis on thinking about what the program has access to, i.e. databases, accounts, etc., and if there could be a way for someone to access these sensitive assets
        - Rather than being able to directly measure this control, there should be tests run to see what a regular user of an application can have access to, both through regular usage and active penetration testing
        - If there are regularly occurring patterns of data being exposed than further measures should be taken
    - Sub Control 18.2: Ensure That Explicit Error Checking Is Performed for All In-House Developed Software
        - This ties into the general duties of QA testers to a degree, but rather simply looking for bugs in performance and functionality there should also be analysis on how on application should be exploited
        - An example could be testing possible values within all inputs in any company software, to check what inputs are being blacklisted and/or whitelisted, and how those inputs are interacting with the program after being submitted
        - Discovering a larger quantity of errors does not necessarily correlate to improved error checking, as it could also be due to a lacking in the development team's performance, however it should at least be noted when few errors are found, as those cases should be further validated to be sure no important areas were missed
    - Sub Control 18.5: Establish a Process to Accept and Address Reports of Software Vulnerabilities
        - This control will help in properly measure the validity of the above controls, to ensure the company's programmers are indeed securing their projects appropriately
        - While there is likely to be many false positives, every report should be treated with proper analysis of its issue, so it can be properly validated and then be given the appropriate response and action to resolve it

        - The number of reports can of course correlate to the amount of issues that are being released when an application is deployed, but more credible can be the rate as to which these reports are resolved, in terms of quantity of resolutions as well as average time it takes to resolve an issue

- Control 20: Penetration Tests and Red Team Exercises
    - This control has a beneficial effect amongst all outlined risks, as in every scenario on of the most important steps to defending against the vulnerability presented, is learning how said vulnerabilities occurs and understanding how it works
    - By establishing where potential exploits originate from, it makes it much easier to create and effective plan against them
    - Sub Control 20.1: Establish a Penetration Testing Program
        - This role should be taken by members within the IT department, who can work in junction with the rest of the company to perform their tests
        - If there is a lack of professionals existing within the company to perform these tests, the company should invest resources into either hiring in-house staff to handle these responsibilities, or even look to third-party vendors to perform these tasks
        - These tests can come in the form more technical assaults on the company's systems and software, to social engineering experiments sent out to company staff, as to see if there are employees who are vulnerable common social engineering attacks
        - By finding out through these tests what methods of penetration are successful for breaching the common will be important data to consider in all other facets of security implementation
    - Sub Control 20.2: Conduct Regular External and Internal Penetration Tests
        - It should of course be assumed at this point, that if these tests are not run regularly, then they begin to lose their efficacy as to how relevant the data acquired from these test will be
        - Tests of the same kind should have their results compared each time they are run as to see if what vulnerabilities are still being discovered, as well as what vulnerabilities seem to be occurring less frequently
    - Sub Control 20.8: Control and Monitor Accounts Associated With Penetration Testing
        - The employees and accounts associated with them will of course have elevated access to company systems and resources in order to perform their tasks

- These accounts should always be verified they themselves do not pose a threat and/or vulnerability, either through the account being compromised by a threat actor, or the employee owning said account having malicious intent themselves
- Similar to keeping records on administrative accounts, these accounts will most likely also fall within that category and should be logged similarly

5. Laws & Compliance

PIPEDA Principles:

- Principle 1: Accountability
    - All departments will inevitably be dealing with some form of sensitive data, either being related to the company, customers, or both
    - Upper management in each department should be aware of what data is moving through their employees, keeping track of who is working on a specific project and what information is included within it
    - If data is breached within a certain area, it can then be tracked to whose hands the data had gone through and appropriate measures can be taken according to the situation by the management in charge
- Principle 2: Identifying Purposes
    - Whenever the company requires certain consumer or employee personal data, it should always come a proper record as to what data is being divulged and for what exact purpose it is needed
    - This can come in the form of terms of service agreements, or outlined in writing within input forms as to what data is being used for
    - Whenever there is an update to how the data is being used or what if new data is required, this should always be sent out through common correspondence to related parties, such as through email
- Principle 3: Consent
    - This ties heavily to Principle 2, as in order for consent to being properly provided there must be transparency as to the purposes of the required information
    - Being a game company, they will likely have a substantial audience of customers under the legal age for proper consent
    - There should always be validation as to the age of individual consenting, or the consent of a valid guardian should they be underage
- Principle 4: Limiting Collection
    - Any analytics or data given to the company must have a valid purpose, whether or not consent is given
    - Measures should be taken to minimize the data required for company functionality as much as possible, and said data should obscured to the company whenever possible, such as through password hashes for accounts
- Principle 5: Limiting Use, Disclosure, and Retention
    - Just as it is outlined when acquiring the data, said data should always be used for the presented purpose and nothing more
    - The company can also keep track of consumers whose accounts related to their games have been in active for an extended amount of time, and can send out correspondence of this to said consumer to affirm their status, in which case if they are no longer using that account the company can proceed with the deletion of its information

    - Similarly for employee credentials and information, if ties have been completely severed with that employee then there should no reason to keep that data
- Principle 6: Accuracy
    - If data needs to be used for a vital purpose, it should always be verified that said data is indeed accurate to its relevant circumstances, especially if incorrect information could have severely damaging results should it be put into use
    - Confirmations should always be in place when it comes to transactions involved with the company, as well as proper validation technology as to ensure the payment information involved is completely accurate
- Principle 7: Safeguards
    - Following the controls outlined previously will help ensure proper security measures are taken around data that goes through and/or resides within the company
    - For some specifics, this can include implementing standardized encryption, properly setting up firewalls, and making sure on-premise locations have physical defenses preventing unauthorized access
- Principle 8: Openness
    - Just as mentioned within Principles 2 and 3, there should be complete transparency as to how any data is handled to related parties
    - Nothing should ever be withheld or misrepresented in regards to policies and agreements outlined by the company
    - Validation of this should be run responsible individuals within the company, the parties/individuals involved with the data, and if needed, third-parties can be inquired as to provide a voice of non-bias
- Principle 9: Individual Access
    - Data should always have a record as to how it was obtained and with whom that data is being held by
    - This ensures high levels of availability and integrity of the data whenever it is needed for a purpose, especially in ensuring the purpose it is being requested for is appropriate
- Principle 10: Challenging Compliance
    - To relate back to Sub Control 18.5, every compliant/report received on an issue should always be processed with proper due care, as to ensure all potential issues are handled appropriately
    - This includes issues received both within the company and from third parties such as consumers and other businesses
    - The sooner an issue is addressed, the less likely for it to worsen and potentially cause immense damages

6. Conclusion

Much of the focus for the chosen controls was given toward resolving the risk around scenario 2, as not only does that present a potential for massive damage to the company, but also proves also a very vulnerable area due to the lack of proper security awareness amongst staff. Controls 4 and 17 especially should have a great effect on patching this weakness and helping reach that desired capability goal. While it may take time to reach the goal of level 5, these controls alone provide much more structure and organization to the system in place, more so due to the fact there currently isn't one, when properly training and mitigating the security threat of exploitable employees at the company. While the other risks presented may have had more infrastructure in place and/or presented lesser risks, these controls should help to further strengthen the security around them. This would especially seem to be the case for Control 18, which should prove to not only lead to more secure code being produced in the company, but should also help the developer in having better mindsets on how they structure their code, hopefully fostering a precedent of continuous improvement around their work. Considering that the IT department still requires more resources to be able to handle the company at its current state, control 20 may be the most difficult at this time to properly implement. That being said, this could be the most vital control to have running, as it can tie into every possible cyber threat to the company, both now and in the future. If necessary it would be worth instead to look to third parties to handle this, as having proper penetration testing would aid in the development of all listed controls. Overall, while there will always be further room to improve, following the outlined solutions in this document would greatly benefit the company in regards to its cyber security, and should be implemented post-haste should plans of expansion continue at its current rate.