Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	Low	Moderate	High
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than 4 % reduction in customers due to loss of confidence	10 to 15 % reduction in customers due to loss of confidence	More than 20-30 % reduction in customers due to loss of confidence
Other:			

Reputation –

Risk Management Criteria – Low

Situation – A minor transaction glitch (financial)

In this situation the issue may arise that there may be a small and temporary glitch in the online payment system of xy innovate and this would lead to certain transactions failing and the impact of this on the company would be customer complaints and inquiries which may lead to an increase in customer services department, and which may lead to potential revenue loss. To delve into the reasons why this may cause financial loss is crucial to state that xy innovate is a financial Technology Company which means that online payments and transactions is at the core of their business model and is the service they provide as a business so breakdowns and glitches even temporary would lead to customers not being able to complete financial transactions which would ultimately impact the amount of revenue we would generate through the flow of revenue that could have occurred in that short period where there was a glitch. Another reason why this may lead to financial loss may be customer refunds, certain transactions may require partial or full refunds, which would place an increase in our workload and expenditure of resources to complete this task. This links in with the PCI DSS Security framework as requirement 12 clearly indicates that A robust policy would include an incident response for glitches and that if they are absent the organization may face chargebacks , compensations and operational costs this is crucial to understand as it tells us that minor glitched are not only an organizational issue however also could be a sign of noncompliance with pci dss.

With regards the issue at hand that the organization may face I have specifically chosen this risk to be low even after referencing the pci dss possible compliance issue more often than not a glitch can be completely accidental and random even if all the correct procedures are in place and with regards to the impact public perception may not be damaged badly mainly due to public knowledge and an acceptance of the fact that minor tech glitch are bound to happen and as long as their transactions are still able to be processed there is an acceptance and level of patience. This is entirely dependent on if the xy innovate is a well-run and efficient organization and based of their procedures and currently we can see that the organization is in a process of improvement as per our knowledge that there was a recent cyber-attack we are also told that there are slight compatibility issue between the updates and improvements to their digital wallet service and the actual banking system this tells us that there may be security flaws which could impact customer transactions in the event of a system glitch however as the businesses is looking to implement the iso framework clause 8.4 is something that the organization should focus on as this point refers to a risk treatment plan and emphasized the importance of having an incident response plan with actions and procedures in place to counterattack and combat the impact if any incidents that may occur. Ultimately, I believe this indicates low risk due to the fact that the possible impact of the this in the case study only included customer complaints and revenue loss and this can easily be avoided it isn’t a deep-rooted organizational issue and with correct procedures in place the risk can be low.

moderate –

Moderate Risk: Lack of Security Awareness Among Staff (~10%-15% Customer Loss)

The situation in this instance would be the fact that employees that are in critical and important roles have not received the best quality of training necessary to complete their job this would increase the risk of small-scale issues and security, privacy and data protection as this is the key processes of the organisation.

Mainly the issues come from the digital wallet services team for example critical team members not being available for an extended period alongside staff conducting tasks outside of their scope. Internal disputes between customer support and software development teams have also not proven effective in mainting and protecting key assets in the organisation. If the working culture of the organisation is not focused on providing staff with the best possible training ultimately the quality of the work produced is going to be weak and in the industry that xy innovate is in a small lapse in quality or service could lead to major impacts on the customers and since this is a common issue across the whole organisation this error could realistically lead to a 10-15 % reduction in customer confidence as this may occur when customers perceive the company in negligent in mainting internal security policies this may garner media and social media attraction if key aspects such as financial loss is included.

The risk levels would be moderate because the inefficient procedures and lack of training and organisational structure can be easily rectified with correct management and internal communication, however if this is not the case then the consequences may result in reputational and regulatory risks. Implementing the iso27001 clause 7.2 which focuses on competence basically states that focusing on staff competence through training would reduce the errors leading to customer satisfaction

High- 3. High Risk: Past Cyberattack

The Situation in this instance that could lead to a high impact score on customer confidence is a cyber-Attack and xy innovate also so have history of having been a victim of a past cyber-attack this was due to vulnerabilities in the digital wallet service which led to key and private customer data being exposed putting the company in a compromised position.

With regards to the recent cyber-attack this is a factual event that has already occurred and has a direct impact on customer trust/loss and reputation the breach exploited a vulnerability in its digital wallet services which lead to a compromise of financial transactions this incident also led to reputational damage alongside a loss of customer trust. Due to this Xy innovate also faced backlash from the GDPR policy as it stated that we would require \ better system in place to handle sensitive financial data. To mitigate the long-term impact that this may have we would need to regain customer trust in our ability to effectively manage sensitive data and financial transactions and to be able to provide a secure and reliable digital wallet service without any risk of technical issues alongside systemic organisations lack of care to ensure the correct procedures are in place

The reason why ive chosen this to be at a high severity is due to many different factors one of them being the long term reputational damage. With potential loss of xy innovate maintaining their competitive advantage in the current market, regulatory backlash and compliance fallouts which include financial penalties the organisation would have to deal with a compounded variety of drawbacks which could potential slow the growth of the business in the market which over time would ensure that we

would lose out on a competitive advantage , customer and revenue which would place the organisation in a difficult position. This would also impact xy innovates ability to raise capital for future investments as their reputation would be damages

Customer loss

Risk Management Criteria Low-

The risk that I have chosen to include in the low customer risk section would be inconsistent customer service responses and this may lead to around 4% customer Loss as highlighted in the risk matrix above.

- Situation: this would be when our customer support team would not be able to provide support to our customers in a timely and effective manner and the reason behind this would be due to the internal communication issue and disputes between our customer support and software development team as mentioned in the xy innovate case study

If we analyse the case study, we can see that the issue is the internal disputes between the software development team and the customer support team this leads to an inability to focus and provide the best quality of support alongside a timeless response to customers that need support. These delays are going to result in customers becoming incredibly frustrated by the delayed response and possibly the incorrect information.

The reason why I have decided to place this at a 4 % or lower customer impact is because of the lack of significant systemic failure that would limit the overall business. With regards to this, the customer support department and process is a segmented and isolated business process and the risk of impact on this department will not necessarily impact other sector of the business such as software etc.. Ultimately for the organisation and especially fin tech companies like xy innovate customers are usually more anxious and on edge when asking reaching out for support because finances are involved in the situation meaning that customers do value when we can respond in a correct and timely manner. On the other hand, if delays become too consistent then this would result in customer loss and customers would stop using our services and opting for other industry alternatives, however this would usually be a small number of customers who are extremely frustrated this can be minimised by implementing the correct guidelines to prevent customer loss. Also due to this department being compartmentalised and only referring to extreme contextual situation it would not directly impact other business departments which would mean we would not lose out on the trust on unaffected customers

I'm basing this percentage of a real-life example of when this occurred to PayPal in 2020, PayPal faced minor transaction delays during the year when using their debit cards to make transactions to platforms such at Netflix etc. Customers were left extremely frustrated and paypal then utilised their engineers and technicians to resolve this issue.

In 2020, PayPal (Paypal 2020) faced minor transaction delays during a system update. These delays primarily stemmed from compatibility and payment gateway errors, temporarily disrupting user payments. While customer satisfaction dipped, the impact was limited as PayPal addressed issues swiftly, ensuring minimal

churn. Studies show that 3%-5% of customers left the platform due to temporary inconvenience, though transparent communication and quick resolutions curbed wider losses.

Customer loss - Moderate

The moderate risk I have chosen that would result in around 10-15 % customer loss would be due to poor policy implementation and compliance issues. To highlight the contextual issue at hand in xy innovate I will reference the following point of concern that may a leading cause in this issue. Firstly, we can see that there has been delayed employee access and account deactivation. What this means is that employees that previously worked at the company would still have access to company information even after they had left. This raises the concern of potential unauthorized access which could lead into the hands of a threat actor. If customers were to be made aware of this they might question the integrity of xy innovates systems leading to a loss in confidence and they may opt for a service that provides better financial security for transactions. This may have a direct legal and regulatory impact as without defined policies the company may be penalised by fines and if this information was to go public for example as was the case with Facebook 2018 data breach where 50 million users' data was compromised this may cause negative publicity that would end up resulting in xy innovate losing out on customers. XY innovate could refer to iso27001 clause 9.3 (management review) to conduct regular reviews of internal policies and to ensure that any gaps are covered to ensure maximum data and access control protection.

High

In adequate safeguards for third party relationships.

XY innovate relies on third party companies such as digital ocean for a cloud storage solution to effectively manage their data and ensure the safety of it on a secured system. As we can see in the case study it has mentioned to us that the contracts with third party individuals do not cover all the necessary security activities which can lead to customer data being at risk of attacks due to vulnerabilities and a system that does not encapsulate total security. Since digital ocean is a large-scale organisation, it increases the complexity of vendor management which would mean that it would become hard to enforce clear communication and security standards as mentioned in the case study there was a lack of focus on critical security measures

As mentioned in the case study there are gaps in the coverage of the cloud solution the issue arrived for the fact that xy innovate store data on servers outside of the country for example in countries such as the USA, Australia and Canada. This may lead to a GDPR issue as concerns may arise with the security and protection of the storage and handling of sensitive financial information. This leads to customer loss since customers are now much more aware of the usage of 3rd party individuals and the risks associated with them due to data breaches such as the 2013 Target Data hack case where the attack originated from third party vendors.

I believe that this risk will pose more of a serious threat to customer loss due to the fact that firstly there will be a clear loss of trust as our customers may see that an over reliance on a third party vendor such as digital ocean may be due to our inadequacies and capabilities to provide the relevant protection this abdication of responsibility creates a sense of distrust in our ability.We could utilise the iso27001 clause8.2 of vendor risk management ensuring that they meet security standards via regular audits and contractual clauses making sure that they are following the correct rules

Allegro Worksheet 2	RISK MEASUREMENT CRITERIA – FINANCIAL		
Impact Area	Low	Moderate	High
Operating Costs	Increase of less than 5% in yearly operating costs	Yearly operating costs increase by _5_to _15__%.	Yearly operating costs increase by more than _____%.
Revenue Loss	Less than _____% yearly revenue loss	_____to _____% yearly revenue loss	Greater than _____% yearly revenue loss
One-Time Financial Loss	One-time financial cost of less than $___$50,000 $150,000_	One-time financial cost of $___$250,000 – $1,000,000__	One-time financial cost greater than $_____$1,000,000_
Other:			

Operating costs Low –

Implementation of basic backup servers alongside office equipment updated.

The reason that these costs would fall into the low section is that small costs such as printer paper, ink, this would be categorized as small incremental investments over time. Xy innovate also utilizes a cloud solution for data management (digital ocean) for data storage and management. This mean that it allows us to not utilize any in house resources to manage this data which intern reduces the upfront hardware costs alongside any maintence, and recovery costs associated to digital storage of data. The costs that would be associated with this would be the cost to increase storage space or adding software updates to the system. Another small incremental cost would be providing physical safety procedures on site i.e. implementing a fire safety protocol as we can see from the case study, this needs to be implemented in the Newcastle office, and this would fit into a small budget and would not cause us too much financial strain. As presented in the Gartner study small incremental adjustments are not to cost heavy on the organization and are extremely maintainable because correct storage of data utilizing cloud providers keeps internal investment at a minimal alongside implementation of safety procedures such as a fire safety measure would be a one of investment and would not be recurring.

Operating costs Moderate –

Investments in security measures / procedures after recent cyber attack

The reason that this cost would fall into the moderate operating cost section is because after the recent cyber-attack XY innovate must invest in new and updated security measures to ensure that this does not happen again. A few methods that the company can implement are purchasing software / hardware such as VPNS, advanced intrusion detection software alongside the correct hiring of specialist cybersecurity consultants that can guide the company to a systemic change in how the company prevents and mitigates the risks of a cyber-attack. Another major cost would be upskilling and training for staff members, i.e. purchasing training content online for staff to complete or dedicate days to upskilling and bringing in training companies to upskill your staff and depending on the level of knowledge required this may be a large step to implement especially if the current level of knowledge held by the staff is low. The research indicates an increase in Global tech spend to reach 2 trillion by 2028 (Forrester 2024) this paper highlights the fact that companies are increasingly investing in security spending to enhance the security of their organizations to ensure regulatory and industry compliance. This indicates that there must be initial investment to bolster the companies' capabilities to protect their assets and this would require a good amount on initial investment and maintence of training and upskilling.

Operating costs – High

Cyberattack recovery cost focusing on the infrastructure shift/ transition to a more secure method.

The recent cyber-attack on xy innovate highlights the issues that were apparent in the organizations key vulnerabilities including weak authorization system and poor security training and methods in place, due to this the cyber-attack led to significant reputational damage alongside penalties in line with the Data protection act of 2018 (GDPR 2018) which has highlighted the requirements for a new way of operating. One way this can be done is by moving to Saas Model over to a on premises or hybrid infrastructure. Now this would be an option to allow XY to innovate more control over critical infrastructure and control over their own assets. on the other hand this approach can be extremely costly as this would require a large amount of revenue to purchase servers, implementing procedures, staff upskilling alongside a disaster recovery procedure. From the case study we can see that the customer data is currently stored with a weak security system, and this would not be adequate for the correct security policies. XY innovate must also

address the internal issue of employee's accounts not being deactivated which can lead to issues with access control and other risks such as threat actors accessing former workers credentials to launch data attacks. Another reason why this cost may be extremely high is that as we have been told in the case study there has recently been a high turnover of staff, and this has delayed the installation of the iso27001 standard, this led to key roles being unfilled. Fulfilling these roles and being the correct individuals would incur a large upfront cost to the organization's am utilizing the Equifax data breach case study to back my point up. As mentioned, the Equifax data breach affected 147 million individuals worldwide exposing Personally identifiable information which is like xy innovate as the digital wallet service was impacted which holds personal financial transactional information. The Equifax case resulted in $575 million in settlements for our xy innovative case study. The GDPR penalties can be parallel to this link to a high-cost impact due to the potential financial burden from noncompliance with the iso27001 regulations

Revenue Loss

Low – less than 3 % revenue loss

The impact cause of this revenue loss that I have chosen is minor transactional issues such as glitches and malfunctions' XY innovate case study tells us that there has been occasional payment disruption that has been caused by compatibility issues between the digital wallet services and banking systems which have led to transactional failures. We are aware that xy innovate have a strong relationship built on trust with their customers which means that when glitches or failures occur this doesn't have a major impact on customer trust and xy innovate ensures that there is always transparency around business process and this due to the fact that these issue result In a small percentage of payment failures does not significantly impact the overall organization revenue. A reason that this may be the case is since xy innovate operate on a SaaS based system this could be attributed to how the organization ensures this revenue loss isn't too extreme in situations where there are glitches or issues. With the Saas system they reduce the downtime by leveraging real time scalability and security features which minimize the transactional failures by being able to quickly respond and mitigate the impact of glitches and payment failures. We can see this is a familiar pattern in the financial transaction industry for example we can look at VISA (Finextra 2023). In 2018 the financial company Visa experienced a payment outage across Europe that lasted for a few hours and stopped people from making transactions due to customer communication and organization trust. The company reduced the impact of this to less than 3 %. This aligns with xy innovate as we can ensure customer trust and if there would be transactional glitches you can effectively mitigate the financial risk by ensuring communication and an effective disaster recovery plan(HCLTec,2024) which can be implemented regardless as a contingency plan.

Moderate revenue loss 3% - 10% revenue loss

The impact cause of this would be erosion of customer trust from transactional issues / Glitches and the loss of major institutional customers. In the xy innovate case study it is been highlighted that there is a lack of focus on providing adequate training on cybersecurity practices e.g. implementation of the iso27001 procedure that was delayed. These factors exacerbate the impact and risk of minor breaches which could result in loss of customers, reputation and finances. One major situation that xy innovate may find themselves in because of this is the loss of institutional clients. What this means is that these are clients

that value compliance due to the nature of their business processes, for example a large national company that utilizes our services if we aren't providing services to an elite standard. These organizations are most likely to review their contract with xy innovate or may reduce or suspend their transactions if our services decline. The loss of key customers' illness has an extreme effect on revenue, more so than if it were smaller customers who were to stop utilizing our services. The reason I have included this in the 3-10 percent revenue loss is since trust issues with high value clients usually significantly impact revenue even if the general customer base is relatively secure. The research backs up my point to show that high value customers value a service based around dependability and compliance. We have been told in the research that financial fraud and issues have a severe impact on trust which in return correlates to reducing customer retention

The example that I am using to back up my point is that of Zelle (Treliant,2024). Zelle were the victims of a major fraud scheme that exploited their services and platform. The victims were tricked into authorizing frequent payments which lead to a loss of confidence a reduced usage of the service. This led to a direct financial impact on partner banks with reduced usage of the services. For Zelle the frequent activity led to a loss in customer confidence in the p2p platform which contributes to revenue loss.

High financial loss-

The point that I have chosen to include is for greater than 10% financial loss in revenue due to competitive loss due to delayed innovation. In the xy innovate case study. As we can see from the case study the company, we can see that there is an organization culture of not innovating and cross departmental collaboration to provide the customers with the best possible service. This has led to issues with customer service and due to the nature of the company being a fintech company customers expect innovation and to receive a cutting-edge product with new capabilities and features in line with new technological advancements and delays or stagnation in this department leads to a loss in customer satisfaction. This can have a significant impact on high value customers especially larger organizations who utilize our services because these organizations utilize our products as a service for their company and they expect our services to streamline their organization and to offer real insightful value in order to gain competitive advantage over their competitors by offering their client base an advanced and modern digital wallet service. Another key point that we can see from the case study is that there is a real need to utilize new and emerging markets that we are currently not operating in and providing our services to these new economies would be extremely beneficial. A recent study by oxford academic (2023) has stated that around 20-30 % of an organization annual growth in fintech comes from consistent and continual product development and providing new and innovative solutions to improve services and products and the opposite would be true that a lack of focus on providing new and innovative solutions would result In a loss of market share. To back up my point regarding stagnation and loss of high value clients I have utilized research from the Federal Reserve center for financial innovation. We have concluded from this paper that companies failing to innovate experience a loss of around 15% or greater yearly due to the loss of high value clients and reduced transitions summarize the reason why this percentage is greater than 10 % is due to the loss of high value clients, reduced engagement from your standard customers and not utilizing new and emerging markets.

One-time financial loss – less than 250,000

From the xy innovative case study we have been told that there has been a delay in implementing the 1S027001 certification for many reasons, e.g. loss of key team members. To address these concerns, the organization must be willing to invest in audits, reviews and understanding where the issues arise from a compliance viewpoint. This can include creating the relevant documentation and internal review alongside

dedicated training programs by bringing in specialist and purchasing the correct tools needed for employee success. The organization can focus on specific security updates that can be done without a large investment i.e. patching vulnerabilities in systems such as access control and authentication protocols to protect against threats. These micro changes do not require company overall and instead focus on utilizing the groundwork and foundations that the company already has in place and improving certain processes. A case study has been conducted on SMES in Portugal and the conclusion that was presented backs up my claim that implementing iso27001 by streamlines documentation and gradual improvements to systems and staff training and key minor improvements such as an effective risk assessment / preparation could cost as little as $50,000 - $150,000

Moderate one-time financial loss – $250,000 – $1,000,000

Providing updates to critical security features

In the xy innovate case study we know that there has been a recent cyberattack which has led to major implications for the business and the organization. We were able to learn a lot about the security procedures that are in place and that need to be implemented, one of them being the gap in the encryption and authentication system. This is to ensure the correct access control to be able to access sensitive information and assets in the organization, i.e. databases, servers and physical location. The organization could invest in multi factor authentication and encryption tools to add to the existing SaaS infrastructure. The recovery and improvements that would be required after a cyber-attack would leave the organization in a position that would require them to invest into improvements i.e. implementing real time threat detection systems to focus on monitoring threats and preventing future breach by taking a proactive approach to cybersecurity threat management. Another key cost associated with the cyberattack would be the budget that the organization would set aside for reimbursement of transactions taken place over the digital wallet service was compromised this procedure would help instill confidence in our ability to provide a reliable service to the customers. The oxford academic paper highlights the fact that mid-sized firms experience a need to invest around $250,000 – $1,000,000 to address key infrastructure concerns post cyber-attack and deployment of new and updated tools such as prevention detection systems, Ai and encryption tools. The study also mentioned that these expenses are proportional and dependent on the size of the organization, that's why ive included this in the moderate range as due to the severity of the issue at hand we would set a budget accordingly.

High One-time financial loss – Greater than $1,000,000

The point I would like to make is a total infrastructure overhaul due to breaches in action of a post breach recovery plan to mitigate the impact and future risk of a cyber-attack. The reason why a hybrid structure migration is so important is since xy innovate place a huge reliance on a Saas Service (Digital Ocean) which is utilized to provide a scalable and efficient method of data storage. As this comes with a particular benefits of data storage, it also comes with security issues such as xy innovate having limited security control over key measures and protocols. This decision to prioritize a more scalable data storage solution has led to the digital wallet service being compromised.

Perhaps the need to develop a hybrid infrastructure model to address key security concerns needs to be implemented. The implementation of this would include ensuring that you have dedicated servers to store sensitive data. Another method would be to implement a cryptographic encryption protocol to protect the transmission of sensitive data and introducing a multifactor authentication procedure alongside with ensuring the security and protection of your network is secure by possibly implementing a network segmentation procedure. The reason that this process can be so expensive is that it involves a huge

overhaul of xy innovates existing IT architecture. This includes purchasing new hardware and integration with the existing system, ensuring a smooth and seamless process to ensure that the digital wallet service is still up and running alongside the relevant training and allocation of resources that would be required to train employees to be able to manage the new system,

The articles from oxford academic (2021) highlights the financial burden that a complete infrasture overhaul costs to move systems to ensure increased security and control. The transitions require huge upfront costs to deal with new hardware, software , system integration and maintenance which can often exceed $1,000,000 which ultimately is what xy innovate would be looking to do to combat the cyber-attack. Overall, even though it may be high in costs it's crucial to mitigate cyber risk to ensure the future of the organization.

Allegro Worksheet 3	RISK MEASUREMENT CRITERIA – PRODUCTIVITY		
Impact Area	Low	Moderate	High
Staff Hours	Staff work hours are increased by less than ___5____% for _____1_to __3_____ day(s).	Staff work hours are increased between ____5___% and _____15__% for ___4____to ___7_ day(s).	Staff work hours are increased by greater than __15_____% for ___8 __to _____30__ day(s).
Other:			
Other:			
Other:			

Staff hours low

Staff hours are increased by less than 5% for 1-3 days

As we are aware, xy innovate suffered a cyber-attack recently leaving the organization in a vulnerable position. The following actions were to be taken, patching vulnerabilities, understanding where the issues arose from and fixing minor issues with the systems and to ensure that an audit was carried out to ensure the correct strategy was set in place to ensure that there were no vulnerabilities left in our system. This had to be carried out by our staff.

Its staff are requiring patching the vulnerabilities and update issues such as access control, which we know is an issue at xy innovate as it revoking staff credentials is something that has not been effectively taken place. The time to complete this would likely be spread across 1-3 days with staff being able to comfortably complete these tasks however there may be a small amount of overtime needed as if staff are working on a critical component towards the end of the day it may be harmful and counterproductive to leave halfway through or at least not completing the task to sufficient level that ensures security. The reason for this section being placed in the low-time section is since most of these tasks are routine and can be done relatively quickly via the correct systems the company did not need to exert many resources apart from staff members being asked to work a few extra hours for a short amount of time.

The information highlighted in the NCSC(2022) guide highlights the significance of mainting a strong cybersecurity posture, this includes ensuing systems that are up to date and the relevant patch of software is being conducted to reduce the disruptions occurred during minor breaches.

Moderate Impact: Staff work hours are increased between 5% and 15% for 4-7 days.

After the cyber breach xy innovate were on the path to implement the iso 27001 framework however this was not completed leaving the organization in an exposed position and vulnerable to attacks. Now the organization needs to implement some key measures of prevention and disaster recovery, this will in return increase the staff working hours. This coordinated attempt needs to involve those across all departments with staff required to work additional hours which would be accredited to deploy new security measures and to educate existing staff on the new policies being implanted and conducting audits on internal reviews and conversation on where staff and individuals feel like there can be improvements. Manual systems to detect anomalies could be handled by current employees until the organization is able to implement a new system of detection and prevention so in short staff would be tasked with maintaining systems and workload that would usually be automated until xy innovate can establish new and updated systems. The study from MDPI(2023) references the point that an incomplete implementation of the iso27001 framework results in the organization increasing the reliance on manual process to cover threats and vulnerabilities which would then result in increased staff hours.

High Impact Staff work hours are increased by greater than 15% for 8 – 30 days

The xy innovate case study shows us that the current digital wallet infrastructure can be compromised and has vulnerabilities as per the recent cyber-attack, a minor glitch in the online payment system caused multiple transactions to fail resulting in customer complaints and revenue loss. Now this can relate to the impact of increased staff working hours since if the organization commits to offering new and innovative digital wallet solutions alongside offering a major rollout of new features such integrating new cryptocurrency features or advanced financial analytics features, this will significantly increase the amount of hours needed by the staff to commit to implement these new features. This would take a joint collaborative effort from departments across the organization such as the IT and product teams who would be ensure that the development and testing of the digital wallet service is correctly implemented and is compatible with the existing system this step would include a quality assurance test. The marketing and communication team would be responsible for ensuring that the correct campaigns are in place including running beta testing programs and gathering customer feedback. The customer support teams would help the users navigate issues and provide support with any questions or technical issues there may be on the user end , this workload for the customer support team would increase significantly from the time of launch around 2-3 weeks past launch to handle the increased workload. The article from HRB presents the idea that in order to implement a successful tech roll out , cross departmental collaboration is required and this would increase the workload for the relevant departments. This argument backs up our claim at XY innovate that the implementation of a new and improve digital wallet service will require more workload from staff to complete.

Allegro Worksheet 4	RISK MEASUREMENT CRITERIA – SAFETY AND HEALTH		
Impact Area	Low	Moderate	High
Life	No loss or significant threat to customers' or staff members' lives	Customers' or staff members' lives are threatened, but they will recover after receiving medical treatment.	Loss of customers' or staff members' lives
Health	Minimal, immediately treatable degradation in customers' or staff members' health with recovery within four days	Temporary or recoverable impairment of customers' or staff members' health	Permanent impairment of significant aspects of customers' or staff members' health
Safety	Safety questioned	Safety affected	Safety violated
Other:			

Life – Low

In this impact situation xy innovates employees do not necessarily Face a direct impact on their health or life but minor issues could occur. Incidents such as slips, falls and spillages may occur within the office. An example we could possibly take from xy innovate case study is that we can see the physical organization of papers and documents on the table isn't the best. From this we can see that the organization of resources aren't efficient or as best as they could be. An issue such as misplaced wire in the office may cause an employee to trip over the cable. This could impact workflow since the worker may need to receive first aid. The fact that the organization is a technical company is more than likely that there would be some components that need correct storage and management, and a loose cable would be one of these. These types of incidents are usually a part of basic health and safety protocols and most likely a critical component of any organization.

Life Moderate –

So, in this instance this would involve an instance when a threat would impact on the health and wellbeing of the customers or of staff that would lead to serious injuries and health issues. An example of this from the case study could possibly be from the cyber-attack and the exposed digital wallet service. This cyber-attack could possibly lead to customers becoming stressed or panic which would threaten their mental wellbeing, this would be understandable if there is a financial risk at stake here to summarize , the outcome of a cyber-attack on the mental and physical wellbeing of individuals involved in the cyber-attack could result in hospitalization or psychological issue through stress , over worked individual's and panic attacks especially for customers and staff with preexisting health conditions. This would also cause possible issues in the workplace and xy innovate would need to implement the correct contingency plan for addressing mental and physical wellbeing.

Life- High

In this instance, this would be when there is a threat or danger that would pose a direct risk to the life of the staff working at the xy innovative offices. As we are told on the case study the fire exits would need to be updated alongside the fire safety policy, this shows us that the security measures in place at this moment in time are not sufficient in complying with the correct standards for office fire safety. An example would be a workplace fire at xy innovate offices due to electrical failure which would lead to a loss in life if the organization were not willing to invest in the correct security methods. The consequences of this would be severe as it would lead to psychological damage and emotional damage to the team, especially if there is a loss in life and the outcome is that it was due to negligence on the organization's behalf. A real-life example would be the 2017 Grenfell tower fire which caused 72 deaths and led to a huge social and political backlash. The similarities are that businesses operating in a high-risk environment must ensure that the correct protection methods are in place.

Health Low –

My impact here would be referring to the impact of the implementation of the ISO 27001 standard and the health issues it may cause. The implementation and adoption of the iso 27001 standard at xy innovate requires a substantial amount of work i.e. implementation of systems, software and compliance. To implement this, employees would be expected to work extended hours and meticulously monitor and handle the implementation process. This increase in workload may lead to minor health issues such as eye strain, Wrist pain and minor skeletal issues such as back / neck etc. due to prolonged hours of programming and reviewing documents and conducting system analysis. The reason why this impact area is relevant in terms of the xy innovate case study is because we are told that the company is working towards implementing the iso standard which involves tasks such as risk assessment, pen testing, and security documentation among various other tasks. This would lead to employees spending a large amount of time sitting at their desk in front of screens and documentation. The impact that it can have on the organization is that it perhaps led to short-term motivation and productivity due to fatigue, this may also lead to increased absenteeism and morale if staff are perceived to be over worked and undervalued. The recommendation would be to ensure you are mandating regular break intervals and perhaps purchase more ergonomic and comfortable seating for staff. The research article from the British medicine bulletin(2021) highlights the fact that sedentary behavior is considered a unique hazard to health and that staff should be taking a good amount of time away from the desk to move and stretch.

Health Moderate-

My impact here would be referring to the impact of the isms and the mental stress / burn out from new and on-going breaches / vulnerabilities. The implementation and adoption of the iso 27001 standard at xy innovate could lead to our specialists' workers simulating data breaches or managing on going data breaches. This could be an intense task which would require a large amount of time and dedication to resolve this, maybe led to mental stress or burnout that may lead to staff needing mental health support. With regards to xy innovation we are aware that there is a significant reliance on the digital wallet service as this is our main business process and asset which means ensuring the security and safety of it is of extremely high priority and breaches could lead to serious issues for the organization. This may lead to staff temporarily making mistakes and errors due to burning out and not being able to correctly focus on the task at hand. This could lead to increased pressure on the actual staff workers to ensure that the task of mitigating and reviewing data breached is conducted on time. The recommended mitigation strategies for this would be to provide stress management support in the form of incentives, whether financial or business-wise.

Health High – My impact here would be referring to the psychological impact of the data breach on the mental wellbeing of staff may result in severe psychological trauma which may be long lasting. The staff may suffer from a sense of guilt if they are managing financial data sensitive information as they may hold themselves accountable for the issue. The xy innovative case study references the dependency that it has on ensuring customer trust and a breach that directly impacts that trust severely may escalate into a much more serious matter for all individuals involved. The impact that this may have on the organization would be employees handing in their resignation due to poor health and burnout to a sever level. This may impact

on organizational reputation and culture as employees are being given a traumatic experience and this may reduce the appetite for other key staff members to work there.

Safety – low impact

When implementing the iso27001framwwork into the business there may be some key issues with regards to privacy and employee safety during the security and privacy updates. An example of this may be the implementation of an internal cctv system to monitor key assets and infrastructure such as data servers. The issue is that employees may feel like their personal space and privacy are being invaded which may lead to a sense of discomfort in the workplace. The impact that this may have on the organization is that employees may not trust the workplace that they are working in and this would lead to a reduced level of moral. We are aware that the company will need to secure the digital wallet data and this may include implementing physical security measures. The mitigation strategy needed for this would be to ensure clear and transparent communication and to explain the benefits of the new security measures to the employees and how this will benefit the entire organization and their job Aswell.

Safety - Moderate impact

When implementing the iso27001 framework into the business there may be some key issues with regards safety for example incidents including moving hardware around the offices and installing equipment. This may cause temporary issues such as blocking the fire exits which would create an unsafe work environment. From the xy case study we know that implementing new hardware involves moving around and installing equipment. This increases the risk of employee safety because there would be items in the office that are heavy and would impede space and in the case of an emergency it would be difficult to move. Besides from health and safety concerns the productivity of employees may dip in the It network department as this will be a section of the businesses where new infrastructure will be included and tested out alongside the Newcastle and London offices. The mitigation strategy would be to enforce clear and effective security measures during the planning stage of this activity alongside making sure that the offices have clear banners and label the hallways and offices that are included and where the hardware will be located.

Safety High –

A high security risk would be a fire occurring the London and Newcastle offices and this would be due to improper cable management and obstruction of fire exists would make this risk even worse this would occur during the implementation of security upgrades to our system. Inadequate safety checks during the implementation of the iso 27001 framework may lead to evacuation delays or injuries during emergencies. From xy innovate case study the implementation of access control systems to protect the digital wallet service may lead to the company not necessarily valuing safety inspection as the priority may be to quickly implement the new system meanwhile not taking not consideration the safety measures that should not be rushed. The reasoning for this would be that due to the nature of the organization and previous history, it is crucial to quickly implement the new systems in order to complete the iso framework and it may be possible that safety of these systems is over looked temporarily to promote speed. The organizational impact of this may be a sever loss of reputation that could erode trust between stakeholders alongside serious legal repercussions. The strategy would be to ensure a rigorous audit is occurring which occurs pre installation and post installation and to ensure that the correct security training is being implemented for staff members

Allegro Worksheet 5	RISK MEASUREMENT CRITERIA – FINES AND LEGAL PENALTIES		
Impact Area	Low	Moderate	High
Fines	Fines less than $_____are levied.	Fines between $_____and $_____are levied.	Fines greater than $_____are levied.
Lawsuits	Non-frivolous lawsuit or lawsuits less than $_____ are filed against the organization, or frivolous lawsuit(s) are filed against the organization.	Non-frivolous lawsuit or lawsuits between $_____ and $_____are filed against the organization.	Non-frivolous lawsuit or lawsuits greater than $_____ are filed against the organization.
Investigations	No queries from government or other investigative organizations	Government or other investigative organizations requests information or records (low profile).	Government or other investigative organizations initiate a high-profile, in-depth investigation into organizational practices.
Other:			

Fines Low – less than $50,000

As we can see from the xy innovate case study the organization has had some difficulty in implementing the iso27001 framework in a timely manner and is now becoming delayed. This tells us that the company is not appropriately maintaining up to date compliance policies and this would possibly lead to low level fines as the actions of the organization do not effectively align with the GDPR article 5 as this policy covers data processing and retention and the organization is keeping sensitive data in the digital wallet exposed as the correct security measures are yet to be implemented. The Impact of this would possible be that regulator such as The Information Commissioners Office (ICO) may decide to investigate xy innovate for their negligence in implementing secure policies to store and ensure the protection of their data which would be done by implementing the iso standard which is being delayed. This exact issue doesn't necessarily involve a data breach however it does show a level of negligence and noncompliance with the GDPR's transparency requirement (article 12) which refers to the transparency of the data alongside article 30 which refers to the record keeping obligations that the company is expected to comply with. To explain this in the context of xy innovate would be that if the organization neglects their responsibility to regularly update their privacy and data protection policy to back up how data should be stored and the access and transparency of that storage then there would occur minor fines. The reason why the potential impact would be low is since this wouldn't necessarily have any immediate impact on our customers, however it would lead to fines for incorrect policies by regulatory bodies, this also can be easily rectified and is relatively straight forward to fix. We are also aware that under GDPR Article 83(4) organizations can be fines up to $10.9 million for minor infractions, for example record keeping errors or the negligence of keeping an up-to-date internal procedure for data protection.

Moderate- $50,000, $500,000

The impact area that I am focusing on in accordance to the xy innovate case study the financial ramifications of the delayed notification of a data breach we know there has been a certain negligence implementing the iso27001 standards if a medium scale data breach occurs and the organization does not report this breach to the relevant regulators within 72 hours then the company would face financial penalties in failure to take proactive action and notify the correct bodies this is in accordance with the GDPR Article 33.The reasons why xy innovate maybe in this situation is that the IT and compliance teams may need more time to understand the issue at hand especially now that the numbers of staff available are reduced due to recent departures from the company. Regardless of the rules stated, the organization must notify the relevant parties within 72 hours even if all the details are known or unknown. The reasoning behind why this may occur and may be an issue is that from the case study we can see the organization over reliance on SaaS providers and limited company resources to understand the security risks and effectively manage them hence why this is outsources which shows its inability to effectively manage its security risk however we can see that they have a dedicated SOC team to maintain a level of security over potential threats however there is a reliance on external 3rd party sources. Other reason for why this would be the case from the case study is the organization of compliance documentation we are told that crucial document are scattered all over the desk in the offices showing us the organization does not value having a structured and organized compliance and documentation filing system and shows a level of unseriousness

and disorganization which could show us their lack of capabilities with handling sensitive data and breaches. This also links in the GDPR article 33 as delayed notification of breaches are usually analyzed to ensure a level of clarity and transparency and to ensure that there is a correct procedure and set of rules to protect people's critical information (PII).

High Fines – $500,000 <

The impact point that I have chosen here is xy innovate incurring significant fines however not because of a data breach related to their digital wallet service however due to a third-party vendor failure which would be due to their significant reliance on SaaS such as Digital Ocean. The situation would be if Digital Ocean failed to meet security standards or were exposed to a lack of data handling procedures and compliance. This would result in regulatory penalties for xy innovate in accordance with the GDPR Article 28. Article 28 ensures that xy innovate are responsible for the actions of digital Ocean with regards to data and privacy compliance. The reasons why this may occur is dure to overreliance on external platforms for scalability and not taking security of the data into consideration. A few ways that this could be achieved would be through data segmentation protocols and placing encryption techniques in place. Digital ocean services may have recently misconfigured their cloud storage system which would have left sensitive data publicly accessible, and this would be an example of how regulators would impose fines on the organization. The fines in this instance would be in line with the scale of the incident and sever to the extent of which xy innovate has neglected its role to ensure the companies that they use are keeping update with data compliance through regular communication and audits of the policies and procedures that they have in place. The example that I am using to back up my point is that of Amazon. On July 16th, 2021, the Luxembourg DPA's fine of $746 Million on Amazon highlighted the strict fines that regulators impose on organization for failing to comply with GDPR policies. What occurred was that on amazon's behalf there was an improper use of customer data for targeted advertising, this backs up my point of data controller responsibility. This would be especially prevalent when there is 3rd parties involved, and sensitive data could be exposed.

Low lawsuit impact –

The scenario in this instance would be that of a minor grievance from customers that would be threatening to file a lawsuit against xy innovate on the grounds of a grievance with the level of security and company procedures on handling data retention policies or security vulnerabilities. The reason why I would place this in the low lawsuits section is that it does not directly involve any actual harm, it's a complaint against our handling of data. The way that this arises is that customers may see xy innovate delaying the implementation of the ISO27001 as a sign of incompetence and laziness and not taking a proactive approach to securing their information, The claim could utilize the GDPR Article 5 principles against the company is a perceived notion that the way the data is stored is outdated or inefficient. The reason this would be classed as low is that during the investigation the regulators would find that there is actually no apparent damage or harm to the customers data, and this is purely an issue of prevention. Customers are legally able to question services and dissatisfaction. Under the Uk consumer rights act of 2015 however in this instance courts are unlikely to provide any compensation as there would be no real damage or impact from xy innovates side.

Moderate – An impact point for a moderate Lawsuit impact point ranging from $50,000 to $500,000 compensation would be that of a failure to provide contractual obligations for the digital wallet service the

partners / clients could claim compensation for delays in implementing relevant updates to the digital wallet service that would be essential for the operation and running on the client's business. These delays, for example a high value client had previously approached xy innovate and asked for a certain compatibility feature between websites to be added to our digital wallet service and thus was proposed as an urgent task. This delay would directly impact on the client's operation and thus leading to a lawsuit against xy innovate with the claim of financial damages and harm to the running of their business. The reason why this would be moderate is because the impact of this action would only be limited to a selected handful of high value clients and not the entire customer base. This type of lawsuit and claims are filed under contract low and the uk consumer rights act of 15 and the unfair contract terms Act 1977 both are relevant in understanding these claims as these policies are used for regulating terms and help to provide solutions and guidance and failure to provide services. Linking this back to the XY innovate case study we are aware of the fact that there has been recent delays in features rollouts and infrastructure improvements that have not yet been implemented as per should be and this means that high value clients that value innovation and a timely response to their needs are likely to take legal action when these dalays impact their business operations and running.

High – A high Impact point for a lawsuit over the value of $500,000

The impact because that would be the reason for this would be due to a possible copyright infringement. XY innovate may be sued for Intellectual infringement by a competitor claiming that the organization have replicated core features of their digital wallet service and implemented it into their own services. The way this issue comes to fruition is that the rival company will claim that xy innovate had recently implemented features that were comparable to a direct competitor. From the case study we can see that A client informed the customer service supervisor, David Bloom, that a competitor hired both John Doe and Jane Smith. This shows us that there may be a possible issue between xy innovate and a competitor as the previous employees of xy innovate may have possible exposed xy innovate to a direct competitor. The reason why I have included this in the high section is because IP infringement lawsuits are extremely intensive and undergo a rigorous process to find any miss doings this includes an extensive audit and this then incudes possible court dates, legal settlements and legal disputes. The claims are most likely to be filed under Intellectual property law such as the uk copyright , designs and patents act of 1998. And if after the investigation xy innovate are found to be in violation of laws then they may face penalties of $500,000 or above. The case study that I am using to back up the claims that I am making is that of oracle vs google. This revolved around the use of Java Api's in google android's platform. the claim by oracle was that of google had implemented the APIs without their permission and thus oracle had faces losses of licensing fees. Oracle has sought to claim $9 Billion in damages. and these examples highlight to us the financial and reputational risk companies face when technology is allegedly used without the correct licensing and regulations. Similarly, xy innovate could face the same backlash if their digital wallet features replicate competitors' property, technology or algorithms.

Investigations- No queries or frivolous request for information.

We are aware that xy innovate does have an intention to implement the iso27001 framework. However, they have been backtracked due to delays, the organization is trying its best to operate with compliance however a customer with a grievance over a bad service may place a complaint or an informal query to a regulator for example the information commissioner's office (ICO), however the issue at hand isn't necessarily serious which means the risk profile is relatively low meaning that to many resources will not be expended to resolve overcome this. The way that this issue arises is that there would be minor grievance with regards to the organization's privacy policy which would eventually lead to an investigation around

data transparency which can be reflected in the GDPR article 13 which is about information that should be provided to individuals. An example in this instance would be that of a customer requesting clarity and information on how their PII information is stored and has concerns around the security of this and then reports it to the regulator. The reason why this would be a low impact risk is due to the fact that the query may not lead to a formal investigation or inspection. However, regulators may get in contact with xy innovate and ask for clarity and additional information. This can also be resolved by editing and updating certain compliance documents.

Moderate Investigation Impact – The moderate impact area of this 3would be that a government body or regulator asks xy innovate to provide them with a specific request such as access to specific records to be able to invest an isolated issues that has been brough to their attention for example noncompliance with data retention policy. The reason this may occur in relation to the xy innovate case study is that a whistleblower may complain to suggest that xy innovate in possession of unlawfully retained transactional data beyond the correct legal limits which may result in an investigation in line with the GDPR article 5 which refers to the principle of data storage past certain times. The regulatory body will then ask xy innovate to provide internal audits, retentions scheduled at dates alongside the relevant data processing agreements that are in place with customers. This risk is directly linked to the xy innovate case study since we already know that there are key issues with regards to staff training and delayed iso27001 compliance gaps. These internal issues could be a factor that goes against xy innovate as they demonstrate the inability to adhere to data processing regulations.

High investigation impact -The high impact area for this section would be that xy innovate is to be a part of a major high profile regulatory investigation due to a systemic noncompliance issue around data processing and handling which would be triggered by a data breach or repeated customer complaints around the same issue without any action taken. The way this occurs is that an event such as publicized allegation of issues such as the mishandling of PII and financial data is made aware to regulators such as the ICO or the European Data Protection Board. Then the regulators would launch a full-scale investigation into these allegations. The regulators would demand Xy innovate to hand over their data policies, the way they handle their data, recent audits and onsite inspection by regulatory Bodies would also require a long and extensive list of documentation as per the GDPR article 58 which means that supervisory authority shall have investigative powers to conduct whatever investigation they deem necessary. The reason why this can be classified as a high impact area is that the investigation would incur major operational disruptions to the organization as it would have to dedicate a large amount of its work force , resources and time to comply with the investigation and dig up documentation and anything else that regulators would require .Another reason why this would be a high impact area would be due to the fact that there is a public facing risk as this investigation would lead to a loss of customer trust leading to reputational loss and harm as if a company is under major investigation most likely the public would avoid utilizing their services especially as this is a digital wallet service which handles key sensitive financial data.An example of this occurring in real life would be that of British airways in 2019, what happened was that the ico investigated British airways after a data breach that affected 420,000 customers and the reasoning behind this was due to systemic flaws and the company was then fined the amount of £20 Million.

Allegro Worksheet 6	RISK MEASUREMENT CRITERIA – USER DEFINED		
Impact Area	Low	Moderate	High
Workforce Crisis and organizational instability			

Low Impact – due to disruptions based on a lack of resources.

The impact point related to this would be that xy innovate would experience short delays and issues due to a lack and shortage of skilled workers and resource constraints.As we can see there have been recent cases of high priority staff member being of sick leaving a shortage of expertise which has then lead to a reallocation of existing staff who are performing tasks outside of the job role leading to short term disruptions in certain day to day tasks that are deemed as low priority. This then creates organizational overreliance on a small team as they would have to perform multiple tasks that they should not even be conducting. This may leave xy innovate in a weaker position in terms of market growth because fin tech organizations would be hiring the most competent and the correct number of staff. The justification as to why this would be classed as low impact is since it would have minimal operational impact on routines such as system vulnerability patching or updating internal documentation. The result of this would mean that some tasks are delayed by around 1-2 weeks. However, majority of the organizational stability is maintained if xy innovate can commit to staff retention and hiring the correct people at the right time.

Moderate – Crucial staff turnover which has led to delays.

In this instance we would be highlighting the fact that key employees that were responsible for the implementation of the iso27001 framework has left the organization mid may through implementation. This leads to serious delays in the implementation of key systems and procedures such as improvements to the digital wallet service and to the iso27001 framework. From the xy innovate case study we can see key issues such as insufficient staff training protocols these factors create a sense of dissatisfaction among employees as they believe that the organization is not providing them with the relevant tools required to succeed. The reasoning as to why crucial staff would be leaving may be because there is limited room for professional development, which leads to staff being overworked and over stressed and they would be juggling a range of tasks at the same time. The justification as to why I have included this in the moderate impact zone is that this leads to project delays. The departure of staff directly impacts on the timeline of the project being implemented and we can see the impact of it on the organization. This leaves the organization susceptible to cyberattacks as vulnerabilities in our digital wallet services are not being patched or improved and this would then lead to a lack in customer confidence as they would question xy innovates ability to deliver on proposed timelines. The most likely outcome of this would be that high priority tasks are delayed for 2-3 months, which would lead to a financial loss as certain high value clients' requirements and needs are missed, and certain deadlines are not met.

High Impact – This would be a mass workforce crisis which would lead to organizational instability. A mass feeling of dissatisfaction would occur among employees resulting in major organizational issues impacting on innovation, compliance procedures which would lead to significant reputation and financial damage. This issue arises when there is a system failure of implementing a strong leadership model across the organization and the departure of team leaders or illnesses would leave the organization without clear structure or guidance. Another key factor in this is that there is an inability to address dissatisfaction and systemic failure. The xy innovate case study addresses the fact that training programs for staff and compliance measures were delayed, and these delays show a lack of prioritization of employee wellbeing and care. The justification as to why this is a high impact point is that the high turnover of staff has a direct negative correlation to the disruption of core operation such as compliance, customer support , new development and innovation and ultimately negatively impacting customers as they are not getting the

upmost quality of service in all aspects of the business. This would lead to major loss in high end clients and services cancellations, Legal and compliance liabilities for failure to meet contractual obligations. The real-life example I am using is that of apples partnership with Foxconn. Apple faced a major global backlash for its supply chain practices. After an investigation was conducted it had found out that there had been poor working conditions and employee dissatisfaction which had lead to reputational harm. Apple then implemented supplier audits and initiated an engagement program to invest in employee wellbeing. This case study shows us the backlash of overreliance on a small over worked workforce as this creates burnout and dissatisfaction and the way we xy innovate could overcome this just like apple did is by conducting employee audits.

Allegro Worksheet 7	IMPACT AREA PRIORITIZATION WORKSHEET
PRIORITY	IMPACT AREAS
6	Reputation and Customer Confidence
5	Financial
4	Productivity
2	Safety and Health
3	Fines and Legal Penalties
1	User Defined

6 – most important, 1 – least important

6 – reputation and customer confidence,

The reason as to why this is the most important point is because the core business model of xy innovate is operating in a fintech environment. To operate in this business market, the organization must establish a strong sense of trust as there is Pii and financial data involved. Customers will need to feel that their data is safe and secure and that they are not at risk of anything being exposed or losing out on finances and a loss in customer trust would result in customer retention rates significantly dropping and reduce the organization's ability to attract high value customers that would bolster finances by receiving lucrative and huge contracts. We can see from the case study that there has been some delay in the implementation of the iso27001 standard and security concerns and issues from an overreliance on SaaS third party services such as Digital Ocean. This makes the organization extremely susceptible to reputational damage as this is something out of their direct control and would be in the hands of digital ocean. The loss of reputation greatly extends from the barriers of just immediate cliental issues. It also impacts on the companies' ability to generate future investments and acquisitions, in the financial tech industry reputation is a non-recoverable asset where trust can be gained but instantly lost over errors and key issues. An example of this is the Equifax 2017 data breach where a loss of reputation can cause extensive and long-term damage

5- financial

The reason that the second most important impact area is financial stability. This is the cornerstone for operation growth and stability. Without finances xy innovate cannot fund the relevant security updates that are crucial to their organization. This will impact their ability to invest into new technology or expansion into overseas territory or markets and in the fin tech world it is crucial that xy innovate has financial health to upscale their business processes and comply with the new changes to a rapidly changing market. The need for financial health is for the following, this would include funding for security updates, employee training and recruitment alongside digital wallet services to ensure that any issues or vulnerabilities are being patched. The organization also needs to ensure that there are enough finances to cover the legal penalties, compensation and compliance fees that the organization may have incurred recently without leaving the organization in a bad financial state. The reason why this is so important regarding xy innovate is that reputational damage often relates to financial loss via claims and penalties. A lack of funds makes it incredibly hard to recover from crises and not having enough financial cover will just make any damage worse to recover from which spirals the organization into a worse situation.

3- Fines and legal penalties.

The reason that this is the third priority is that fines for noncompliance are usually serious and incur serious damage to reputation and finances. However, in some instances they are negotiable and manageable, especially if the severity of these breaches is low. They can be prevented and managed by taking prompt corrective actions such as improving their security service and patching vulnerabilities and other issues that may be the cause of the claim in the beginning, i.e. lack of compliance documentation. XY innovate would need to implement the GDPR policies.

4) Productivity The reason why productivity is the fourth priority is since productivity is the cornerstone of any organization without the staff completing the tasks nothing would get accomplished in the organization. If the foundation for meeting deadlines , providing content , delivery product and services and providing a quality digital wallet service to the customers' reason that it is ranked at 4 below trust and finances etc. is that any concern with productivity can be easily managed and corrected near instantly whether it be by staff meeting , training or new staff hires and replacing the old staff the organization are in complete control over the productivity rates of their staff. Usually this can be achieved with correct resource allocation and project management to create a much more positive workplace where staff feel enticed and rewarded for their hard work. We can see that this point is a concern for xy innovate as per the case study as we know that the delayed iso27001 certification process and in gaps in key skills that have been highlighted have led to productivity issues for the organization as innovation has been reduced and limited. This will lead to missed deadlines for key projects and client needs.

5) Safety and health

The reason that this is in fifth is that employee wellbeing is crucial and extremely important however health concerns such as employee burn out and stress from being over worked does not necessarily have a direct impact or a large enough impact on xy innovates financial health or its relationship its client's and business partners as other key priorities such as reputation would have. From the case study we can see that the loss of key members and dissatisfaction have impacted the organisation however this issue does not directly disrupt key operations or client relationships until the issue of employee dissatisfaction increases to an unmanageable point.

6) User defined risk (lowest priority)

The reason that I have placed this at the bottom of the risk table is to do with the fact that these factors are usually quite flexible and context dependent. These issues relate to innovation or scalability, and they can usually be reacted to or developed through strategic planning. While these risks are relevant they are not as immediate or urgent to customers trust , financial health or compliance and issues such as stability and delayed feature rollouts are more long term issues.

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
The critical asset that we will be looking at is the customer database	This asset is a crucial foundation of xy innovates digital wallet service which is also essential for our business model. Accidental / intentional deletion, modification of the data alongside unauthorized access can lead to the publication of private data online which would result in damage to customer trust, it would violate the regulatory industry standards such as GDPR. Breach of this would then result in financial loss due to possible breaches of regulatory standards.	Technical asset – This asset comprises of a technical composition as there is financial records stored alongside transaction logs and Pii information which is stored on the Digital Ocean cloud platform. The asset is highly sensitive, and this requires a level of end-to-end encryption during the application and processing and transmission of the data.
(4) Owner(s) *Who owns this information asset?*		
The Digital Wallet Software Services Manager – Nisha Kuar , Supervisor Information Security Chloe Davis , Exec.Vice-President Jamie Lee New Castle , President Alex Turner London		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	The software development IT Team alongside the head of the IT / development team would be required to manage this. The controls in place would need to provide a level of data encryption which ensures only authorized individuals can access sensitive information. To implement this there should be a layer of MFA and role-based access controls.

❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	The wallet Application developers and the database administrators would be responsible for managing this control Only authorized individuals would be permitted to access critical information to modify or utilize. Audit logs should be implemented and updated to represent the most UpToDate information present in the organization. Automated integrity checks can be implemented
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	The Head of The It Team – Supervisor alongside the software development team should be able to access our digital wallet service infrastructure 24/7 and the data administrator should be able to access this during the office working hours
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	Asset should be available for the duration of the working hours; The software developers should only have additional access when a change or update is required to be implemented, and they require a onetime sign on access.
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	So, this should comply with PCI DSS and GDPR Requirements. Alongside the relevant data protection laws of the country. Regular security audits and penetration testing will help us identify vulnerabilities and improve our security measures.

(6) Most Important Security Requirement

What is the most important security requirement for this information asset?

☑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Confidentiality- Given the fact that xy innovates main line of business is providing users with a secure financial payment option via their online digital wallet service, data confidentiality would be the most important clause in managing. A breach of customer financial and personal data would have the most severe impact, which would include legal clarifications and reputational damage. If in a data breach customers, data is exposed, and the investigations show a lack of proactiveness on behalf of xy innovates dedicated team, then the financial impact would be much higher as during the proceedings a case of negligence would be used, and the penalties and impact would be much larger resulting in more fines. Alongside this ensuring a sense of confidentiality would build up customer trust and this is a crucial part of growth in an industry predicated on trust.

Allegro Worksheet 9a	INFORMATION ASSET RISK ENVIRONNENT MAP (TECHNICAL)	
INTERNAL		
CONTAINER DESCRIPTION		**OWNER(S)**
1. Database servers – This is the server hosting the database which contain the primary key financial customer information		The Digital wallet Services Team
		The IT Tean
2. Application Backend – This is referring to the back-end systems that process customer transaction. This interacts with the database and manages the data's integrity		Digital wallet service team
3. Internal Network – This is a secure network transmission between systems to facilitate communication		IT Team
4. Employee Laptops and Workstations – this would be the devices used by employees to ensure that there is a secure way to access databases, customer queries and to perform administrative tasks.		Administration Team
EXTERNAL		
CONTAINER DESCRIPTION		**OWNER(S)**
1. Cloud Storage (Digital Ocean) – Cloud infrastructure which hosts key customer financial data and allows for scalable data storage solutions		Digital ocean service provider
2. Payment Gateway Service – This is an external service that manages secure customer data.		3rd party Payment Gateway Provider
		Finance Team –
3. External Network (internet) – this is the public network which enables the customers to access the digital wallet platform and allows them to transmit data and utilize our platform and services.		It Team
4. Regulatory Systems – This is the system used for reporting and managing the compliance of the organization		Regulatory Authorities
		Administration Team

Allegro Worksheet 9b	INFORMATION ASSET RISK ENVIRONMENT MAP (PHYSICAL)	
INTERNAL		
CONTAINER DESCRIPTION		**OWNER(S)**
1. The Central Server room in the Newcastle headquarters office – we know that this is in the software office in Newcastle and mike Rodgers supervises the software development team so him and the IT team would be responsible for managing the central server room		Managed by the IT Team
		Also managed by the Digital Wallet Services Team
2. Central File Server		The Head Office Team – London
		Digital Wallet Software Services Team – (Manager Nisha Kaur)
3. Employee Desktops and Laptops		Administration Team
		IT Team
4. Meeting and collaboration space in the offices		The Administration team.
EXTERNAL		
CONTAINER DESCRIPTION		OWNER(S)
1. Digital ocean cloud data center – this is the facility where customer financial data and transactional records will be stored		Third party provider, digital ocean
2. Payment Processing -This control is to manage external payment processes		Administration Department - Finance Manager Micheal Wilson
		Accounts Team
3. Archival storage Location – this is the third-party storage facility where data can be transmitted to and analyzed		Administration Team – Accounts manager
4. Digital ocean cloud Data backup facility – this is a separate geographic backup location for the data.		Third party provider, digital ocean

Allegro Worksheet 9c	INFORMATION ASSET RISK ENVIRONMENT MAP (PEOPLE)
INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	**DEPARTMENT OR UNIT**
1. Chloe Davis – This individual is responsible for overseeing and managing the implementation of security measures for the critical assets in our organization	Information Security (IT Team)
2. Micheal Clark – This individual is responsible for managing xy innovates network infrastructure and ensures that individuals have access to the data in a secure and authorized manner	Network Supervisor
3. Nisha Kaur – This individual is responsible for the oversight of the software development process and ensures we are meeting regulatory and compliance standard with regards to the use, protection and storage of critical customer data.	Digital Wallet Software Services Manager
4. Taylor Jack – This individual is responsible for the analysis of critical and sensitive customer data and to ensure that this is managed and utilized in a safe and secure manner when we are analyzing and reporting on data.	Data Analyst (Digital Wallet Services Team)
EXTERNAL PERSONNEL	
CONTRACTOR, VENDOR, ETC.	**ORGANIZATION**
1. Cybersecurity Consultant – this external individual would help Chloe Davis (information security supervisor) with risk assessments and vulnerability management of critical organizational systems.	External cybersecurity contractor.
2. Cloud Services Administrator- this individual would support our usage of their digital ocean cloud platform to ensure secure access of cloud-based data and solutions for storage of information and operational use.	Digital Ocean
3. External payment Gateway specialist – this individual would support our transactional processes and ensure that customer transactions on the digital wallet application are secure.	Third part Payment Processes.
4. Transaction and data storage manager – this individual would support Tom Knowles (The internal audit supervisor) with the processing and secure archival of regulatory compliance documentation and audit logs	**3rd Party Storage Vendor.**

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk / Threat	Information Asset	Digital Wallet financial service	
	Area of Concern	*The area of concern would be unauthorized access to sensitive and private customer financial information (as a recent breach targeted a vulnerability in the digital wallet service) which resulted in compromises of personal data and financial transactions.*	
	(1) Actor *Who would exploit the area of concern or threat?*	Unhappy current employees that are unsatisfied with the way the company is being run	
	(2) Means *How would the actor do it? What would they do?*	This internal threat would be actioned by the means of shared credentials and insufficient access control mechanisms or accessing stored data in from the servers in the Newcastle offices	
	(3) Motive *What is the actor's reason for doing it?*	Revenge on the organization for poor working conditions and ongoing disputes for better employee rights and conditions.	
	(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ☐ **Destruction** ☐ **Modification** ☐ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	A sense of confidentiality, so data was access via weak encryption and storage of Pii on the digital wallet- There should be implementation of the correct access controls in place to limit access to certain individuals.	
	(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High**	☑ **Medium** ☐ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Reputation and customer confidence will take a significant hit as we already have been told in the xy innovate case study. For a fintech company individuals trust our capabilities in safeguarding data and if we are not able to do this it creates a sense of mistrust, and this would lead to a loss in users as individuals would opt for an alternative reducing. A loss in customers would impact on our finances significantly.	Reputation & Customer Confidence	High	12
	Financial	Medium	7

	Productivity would be hindered as services downtime during breaches and the audit / investigation that would be undertaken would hinder the day-to-day running of the organization as the focus would be on the investigation and understanding where the vulnerabilities came from, and this would include meetings and discussions.	Productivity	Low	2
		Safety & Health	Low	2
	Exposure of customers Pii and financial data would lead to possible fines for failing to comply with the 1so27001 and GDPR regulations especially as the nature of the business is processing financial information	Fines & Legal Penalties	High	12
		User Defined Impact Area		
			Relative Risk Score	**35**

	Relative Risk Score

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
❑ **Accept**	❑ **Defer**	☑ **Mitigate**	❑ **Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Digital Wallet Service (Administrative)	• Implement a RBAC (role-based access control) for access to sensitive data to mitigate the risk of anyone internally accessing and exploiting this data, this was if RBAC is implanted and there is a breach there would be a limited number of candidates who would be responsible which would help our investigation. • Conduct regular audits of the digital ocean infrastructure to ensure there is a level of compliance with iso27001 and a sense of computability. This control would help to gain a better understanding of where issues may arise from allowing a better plan of action.
Physical Locations (Offices) (Physical Controls)	• We would implement a sense of restrictions and access to the Newcastle office to ensure that the servers and systems stored there are well looked after and additional security measures such as biometric access and CCTV would be implemented. • We would improve and invest in an offline back up system to ensure that critical data is constantly backed up even if there is a power breach or issues. This means that customer data will always be secure and backed up in its original form. • Ensure that digital oceans relationship and data stores are secure and in a non-vulnerable state

Internal operating system (Technical controls)	• We would implement increased and more secure levels of encryptions such as cryptographic protocols in place such as using AES-256 which ensures that the data has not been manipulated or tampered with • We should implement a layer of MFA especially for those employees accessing sensitive data especially in the IT and digital Wallet Team.
Residual risks	• Zero Day Exploits – so even though we would mitigate threats by conducting regular reviews and analysis deep rooted vulnerabilities in the software or operating system may still pose a threat • Insider threats may still pose an issue if the issue is with employees at a high level of access rights and if they were the individuals responsible for the breach • Cloud dependency – a sense of over reliance on the digital cloud platform would cause a risk if this system was to face downtime.

Threat Scenario Questionnaire 1	**Technical Containers**		
This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation where an outsider could access one or more technical containers, *accidentally* or *intentionally*, causing your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Threat Scenario Questionnaire – 1 (cont)	**Technical Containers**

Scenario 3:

In this scenario, consider situations that could affect your information asset on any technical containers you identified. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

- Unintended disclosure of your information asset
- Unintended modification of your information asset
- Unintended interruption of the availability of your information asset
- Unintended permanent destruction or temporary loss of your information asset

A software defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
A system crash of known or unknown origin occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Ye (interruption)**	**Yes (loss)**
A hardware defect occurs	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Malicious code (such as a virus, worm, Trojan horse, or back door) is executed	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Power supply to technical containers is interrupted	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Problems with telecommunications occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Other third-party problems or systems	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Threat Scenario Questionnaire – 2	**Physical Containers**

This worksheet will help you to think about scenarios that could affect your information asset on the physical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.

Scenario 1:

Think about the people who work in your organization. Is there a situation in which an employee could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Scenario 2:

Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could access one or more physical containers, *accidentally* or *intentionally*, causing your information asset to be:

Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

Threat Scenario Questionnaire -2 (cont)	**Physical Containers**

Scenario 3:

In this scenario, consider situations that could affect your physical containers and, by default, affect your information asset. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:

- Unintended disclosure of your information asset
- Unintended modification of your information asset
- Unintended interruption of the availability of your information asset
- Unintended permanent destruction or temporary loss of your information asset

Other third-party problems occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	**No**	**Yes (disclosure)**	**Yes (modification)**	**Yes (interruption)**	**Yes (loss)**

Threat Scenario Questionnaire – 3	People		
This worksheet will help you to think about scenarios that could affect your information asset because it is known by key personnel in the organization. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.			
Scenario 1: Think about the people who work in your organization. Is there a situation in which an employee has detailed knowledge of your information asset and could, *accidentally* or *intentionally*, cause the information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Modified so that it is not usable for intended purposes?[1]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Interrupted so that it cannot be accessed for intended purposes?[2]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?[3]	**No**	**Yes (accidentally)**	**Yes (intentionally)**
Scenario 2: Think about the people who are external to your organization. This could include people who may have a legitimate business relationship with your organization or not. Is there a situation in which an outsider could, *accidentally* or *intentionally*, cause your information asset to be:			
Disclosed to unauthorized individuals?	**No**	**Yes (accidentally)**	**Yes (intentionally)**

[1] This case is unlikely, but if a key person in your organization has detailed knowledge of an information asset and communicates this information in an altered way that affects the organization, a risk could result.

[2] This case is about the availability of the information. If a key person in the organization has detailed knowledge that is vital for a business process and is not accessible or available, the information may not be usable for the purpose intended, ultimately impacting the organization.

[3] If a key person in the organization knows the information asset and leaves the organization, and the information is not documented elsewhere, it could pose a risk to the organization.

Aristosourcing. (n.d.). The Apple-Foxconn Partnership: A Paradigm of Outsourcing Excellence. Medium. Available at: [The Apple-Foxconn Partnership: A Paradigm of Outsourcing Excellence | by Aristosourcing | Medium]

PayPal Community, Year. Solved: PayPal payments failing. *PayPal Community*. [online] Available at: <PayPal Comes to A Screeching Halt for Some 3P Sites and Plug-ins - EcommerceBytes

Solved: PayPal Payments Failing - PayPal Community

> [Accessed 1 December 2024].

HCLTech. (n.d.). 'Understanding cloud outages: Causes, consequences and mitigation strategies'. Available at: [Understanding cloud outages: Causes, consequences and mitigation strategies | HCLTech

] [1st December 2024].

"When Digital Payments FAIL : Over-Reliance and Real-World Examples | PART 1": By Mahesh Pawal

Treliant. (n.d.). 'The Underestimated Threat: Zelle Fraud's Impact on Regional Banks in the United States'. Available at: [The Underestimated Threat: Zelle Fraud's Impact on Regional Banks in the United States - Treliant

(PDF) Financial Fraud and Credit Risk: Illicit Practices and Their Impact on Banking Stability

] [1st December 2024].

The Oxford Handbook of Banking. (n.d.). 'Technological Change and Financial Innovation in Banking: Some Implications for FinTech'. Oxford Academic. Available at: [How Valuable Is FinTech Innovation? | The Review of Financial Studies | Oxford Academic

Technological Change and Financial Innovation in Banking: Some Implications for FinTech | The Oxford Handbook of Banking | Oxford Academic

] [1st December 2024].

'Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal'. Available at: [Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal

] [1st December 2024].

Journal of Cybersecurity. (n.d.). 'Examining the costs and causes of cyber incidents'. Oxford Academic. Available at: [Examining the costs and causes of cyber incidents | Journal of Cybersecurity | Oxford Academic

] [1st December 2024].

Journal of Cybersecurity. (n.d.). 'Examining the costs and causes of cyber incidents'. Oxford Academic. Available at: [Innovating Big Tech firms and competition policy: favoring dynamic over static competition | Industrial and Corporate Change | Oxford Academic

] [1st December 2024].

NCSC.GOV.UK. (n.d.). 'Maintaining a Sustainable Strengthened Cyber Security Posture'. Available at: [Maintaining a sustainable strengthened cyber security posture - NCSC.GOV.UK

] [1st December].

'The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector'. Available at: [The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector

] [1st December 2024].

Vihini, H., Colombage, R., and Li, X. (2021). 'Information security management: A systematic literature review of digital forensics and cybercrime investigations'. British Medical Bulletin, 137(1), pp. 42-57. Available at: https://academic.oup.com/bmb/article/137/1/42/6168546 [Accessed Date].

General Data Protection Regulation (GDPR). (n.d.). 'Article 12: Transparent Information, Communication and Modalities for the Exercise of the Rights of the Data Subject'. Available at: [Art. 12 GDPR – Transparent information, communication and modalities for the exercise of the rights of the data subject - General Data Protection Regulation (GDPR)

[1st December 2024].

General Data Protection Regulation (GDPR). (n.d.). 'Article 30: Records of Processing Activities'. Available at: [Art. 30 GDPR – Records of processing activities - General Data Protection Regulation (GDPR) [1st december 2024]

General Data Protection Regulation (GDPR). (n.d.). 'Article 83: General Conditions for Imposing Administrative Fines'. Available at: [Art. 83 GDPR – General conditions for imposing administrative fines - General Data Protection Regulation (GDPR)

] [1st December 2024].

General Data Protection Regulation (GDPR). (n.d.). 'Article 33: Notification of a Personal Data Breach to the Supervisory Authority'. Available at: [Art. 33 GDPR – Notification of a personal data breach to the supervisory authority - General Data Protection Regulation (GDPR)

] [1st December 2024].

Data Privacy Manager. (n.d.). 'Luxembourg DPA Issues €746 Million GDPR Fine to Amazon'. Available Luxembourg DPA issues €746 Million GDPR Fine to Amazon – Data Privacy Manager] [1st december 2024].

General Data Protection Regulation (GDPR). (n.d.). 'Article 28: Processor'. Available at: [Art. 28 GDPR – Processor - General Data Protection Regulation (GDPR)

] [1st december 2024].

Supreme Court of the United States. (2021). 'Google LLC v. Oracle America, Inc., 141 S. Ct. 1183'. Available at: [Google LLC v. Oracle America, Inc.
] [1st december 2024].

BBC News. (2020) *British Airways fined £20m over data breach*. Available at: https://www.bbc.co.uk/news/technology-54568784 (Accessed: 1 December 2024).

Aristosourcing. (n.d.) *The Apple-Foxconn Partnership: A Paradigm of Outsourcing Excellence*. Medium. Available at: https://medium.com (Accessed: 1 December 2024).

Aristosourcing. (n.d.) *The Apple-Foxconn Partnership: A Paradigm of Outsourcing Excellence*. Medium. Available at: https://medium.com (Accessed: 1 December 2024).