Gruppe 4
Kandidatnummere: 2, 7, 34, 293, 382, 450

Table of contents

Assignment 1: IS Project Idea

Case: Disaster recovery, business continuity and infrastructure implementation

Nowadays it's basically common to hear about technical failures and cyberattacks that target large companies who are dependent on fast and efficient business models. By implementing disaster recovery and business continuity for companies like Apple. Who have offices globally with a wide range of powerful data centers spread across the world. Apple is financially dependent on handling millions of transactions daily, if the company was to experience a disaster it would surely result in a major financial loss. We would therefore like to implement a disaster recovery and business continuity program.

Infrastructure Implementation is the foundation companies use that depends on services and operations. The CIP which stands for Collaborative for Implementation Practice defines Infrastructure implementation as components of infrastructure that ensure the development of skilled staff, strong systems and organization.
There are two drivers that are vital for this:

1. *Competency drivers*
   Competency drivers ensure the staff have the knowledge and skills to implement changes that are high in quality.
2. *Organizational drivers*
   Organizational drivers see to it that support and resources match the staff needs.

Goals:

1. *Minimum disruption*
   - By making recovery time as short as possible, the company can ensure that their stocks aren't significantly damaged.
2. *Protocols*
   - By regularly having backups that are specifically scheduled for certain times the company can ensure that their systems are up to date.
   - We can also implement accessed based control to limit who has access to sensitive data.
   - A multi-factor authentication just for one extra layer of security.
   - As soon as there is an attack, a notification should be sent out to all employees to halt their actions.
3. *Training staff*

    - By training the staff on disaster recovery we can educate them to recognize any attempts of a malicious threat to the systems.
    - By regularly having drills that are controlled, we can really learn of efficient ways to keep our staff up to date with protocols/training.

SWOT Analysis:

Strengths:

- Scalable Infrastructure
    - Potential to market and sell the solution to other organizations
- Improved security, rapid and better response time on possible cyberattacks.
    - Leads to reduction of downtime
- Improved data redundancy
    - Having multiple datacenters can reduce the risk of permanent data loss
- Cost saving in the long run
    - Initial setup cost might be high, but in the long run the system can minimize the financial impact of an attack that leads to downtimes and other data breaches. The company Maersk is a good example of why.
- Training of employees can lead to better confidence and productivity.
    - Employees are more confident on resolving the problems and stress might be reduced during incidents when having a well defined strategic recovery and continuity plan.
- Increased business reputation and trust
    - Having a strong continuity system and a secure infrastructure will build up the trust for customers, partners and stakeholders. It tells them that we are prepared for incidents.

Weaknesses:

- High initial setup and implementation costs
    - Investment in infrastructure, training programs, and security measures requires significant upfront capital
    - Requires a high level of technical expertise and planning.
- Resource intensive maintenance
    - Requires dedicated IT staff and ongoing training to keep systems and protocols up to date.
    - Requires continuous monitoring, testing and updating to ensure that we are protected on evolving and possible new threats.
- Complex and time consuming implementation process
    - Integration with existing systems and training of employees can be time consuming
- Dependency on Third-Party providers

    - The system might rely on external cloud or infrastructure providers if we don't implement our own cloud

Opportunities:

- Partnering up with cloud service providers to minimize the cost of opening our own data centers
- Develop a standardized solution that could be offered to other companies to gain income and scale the the business

Threats:

- New malware we have not seen before that might be able to bypass our defenses.
- Natural disasters or war that we can't control which can impact our databases. That's why we need multiple datacenters in different regions.
- Competition from already established firms and solutions that could affect and limit our market opportunities.

Technical skills required for this project:

Cybersecurity:
Successfully developing a disaster recovery and Business Continuity System plan requires a wide range of technical skills. Cybersecurity expertise is among the most critical for responding to cyberattacks. Threat detection, incident response, and implementing good security measures to protect the system against cyberattacks.

Cloud computing:
Furthermore, cloud computing skills are important for implementing backup and redundancy planning. Experience in using cloud services like Google Cloud, AWS, or other platforms is vital because they provide the necessary infrastructure to host data centers and ensure high availability.

Business Continuity Management:
It is important to have personnel familiar with the ISO standard, such as ISO 22301 the international standard for Business Continuity Management Systems (ISO, 2019). This ensures that the system is compliant with international best practices and regulations.

Disaster recovery planning:
Additionally, having a member of the team with experience in developing disaster recovery and incident response plans would be a key component for this project to be successful. Their experience will help the project run smoothly by covering the key areas.

Reference:

Cadle, J. & Yeates, D. (2008). *Project management for information systems (5th ed).* Pearson Education Limited 2008

Assignment 2: Business case

Introduction and background
On a day to day basis, businesses are facing a constant threat of cyberattacks and other critical disruptions that can impact the businesses operations severely. These types of disruptions can range from, hardware failures, natural disasters, war, cyber threats and even human errors. In 2017, MAERSK fell victim to a devastating cyberattack that cost them approximately $300 million in damages in only two weeks (LA Times, 2017). The attack disrupted their global operations for weeks, impacting numerous companies that relied on Maersk for shipping their products. This highlights the importance of having a robust disaster recovery continuity system. Therefore, we propose establishing a dedicated department for disaster recovery and business continuity management.

Management summary
This document presents a business case for implementing a disaster recovery and business continuity plan, which is supported by modern infrastructure. The goal is to ensure the organization can withstand any cyberattacks and technical disruptions, minimizing downtime and financial impact.

What:

- This project involves implementing and designing a robust disaster recovery and business continuity plan. This includes developing infrastructure, establishing backup systems, and ensuring critical operations can continue during and after incidents with strict protocols. By learning from incidents like the MAERSK cyberattack, we can better prepare ourselves to handle similar incidents or and other challenges.

Why:

- There are several key benefits of implementing a disaster recovery and business continuity solution:
    - Faster recovery: Reducing recovery time from cyberattacks or technical failures minimizes the impact on company operations.
    - Financial protection: Rapid recovery prevents significant financial losses, as demonstrated by the MAERSK incident.
    - Staff readiness: Training staff to handle incidents improves overall company response time.
    - Trust and reputation: A robust and solid strategy enhances the company's reputation among customers, partners, and investors.

Cost:

- The initial cost will be high, covering infrastructure setup, security enhancements, staff training, and a department for continuous monitoring. Although these setup costs are significant, the long-term benefits and financial savings from reduced downtimes, increased operational efficiency, and lower risk of data loss can outweigh the upfront expenses.

Timeline:

- Estimated time of getting the infrastructure and system up and running is expected to take 12-15 months.

Problem
This project aims to reduce the frequency of technical failures, cyberattacks and other disruptions that may arise to make sure that the business and infrastructure is secure. Based on this we have come up with four possible ways of ensuring this.

- **Option 1: on-premises infrastructure**
  While effective this can be very demanding in the longer run, it requires high capital expenditure and a full department that works around the clock.

- **Option 2: Cloud infrastructure**
  By choosing this option, all systems, data, storage and much more gets migrated to a cloud platform, like google cloud or Amazon web services. This would result in a lower disaster recovery time. This will also bring problems like data security, since there would be a huge reliance on using these cloud services and risks of breaches.

- **Option 3: On-premises and cloud based (recommended)**
  This is the most reliable way when it comes to cost. By having on-premises we can focus on disaster recovery, and situational training. While with cloud-based infrastructure, we can guarantee faster recovery and greater focus on security by encrypting data, implementing multi-factor authentication and regular vulnerability assessments.

- **Do Nothing (Maintain the Current Infrastructure)**
  This option involves making no changes and continuing operations as normal with the current setup. No additional cost or resources are needed and will avoid disrupting any current operations.

Based on these options, we highly recommend going with Option 3,The on-premises and cloud based infrastructure implementation option offers a great amount of strength by combining these two infrastructures together. Mainly by ensuring a quick recovery and stronger security. This investment may seem like a lot, but a key factor here is that this is a long term investment that definitely can yield positive results.

Description of problem or opportunity:
By not having a dedicated department for disaster recovery and basic It security the organization is at great risk. Cyber threats are rapidly growing and becoming more sophisticated and frequent. The result of a cyberattack could lead to major financial losses, data breaches and harm to the company's reputation.

Additionally, nowadays it is almost mandatory to have proper IT security measures in place to meet industry standards. Regulations like ISO 22301 emphasize the need for disaster recovery and business continuity. Failure to comply with these standards could result in fines or penalties.

Improved security and rapid response:
As mentioned earlier in the SWOT analysis under strengths, a dedicated disaster recovery team would improve security and reduce downtime during cyberattacks. In today's landscape of growing cyber threats, being able to respond fast is crucial for business continuity.

Data Redundancy and risk reduction:
Setting up multiple data centers will help reduce the risk of permanent data loss. This will ensure that critical data remains secure and is accessible during incidents.

Trust and reputation:
Implementing a good disaster recovery department can result in better reputation and build trust with the customers and stakeholders.

Long-Term investment:
While the initial investment may seem like a lot, implementing a disaster recovery department would be of extreme value. It will reduce financial losses in the future by ensuring a faster recovery from an incident. According to the IBM Cost of a Data Breach Report 2024, the global average cost of a data breach in 2024 was $4.88 million (IBM, 2024, p. 8). This shows why taking action early is important.

Options available and considered
Option 1 provides tighter security with on-premises hardware but comes with higher costs and risks of physical disasters. Option 2 offers a cost-effective cloud solution with scalable resources but has potential data privacy concerns. Option 3 combines the strengths of both on-premises and cloud solutions for enhanced disaster recovery

but involves higher complexity. Option 4 considers doing nothing, maintaining the current infrastructure without additional investment.

Option 1: Physical Hardware On-Site
This option involves investing in physical hardware that is stored and maintained on-site, ensuring tighter control over data and security protocols.

Pros:

- Higher security due to on-site hardware control
- Reduced risk of third-party breaches

Cons:

- High upfront and maintenance costs
- Increased vulnerability to natural disasters (flood, fire, etc.)

Costs:
Significant initial investment for hardware and ongoing maintenance expenses.

Feasibility and Scalability:
Suitable for organizations prioritizing data control and security. Limited scalability due to physical infrastructure.

Recommendation:
Not recommended unless the organization has a critical need for on-premises security and is willing to bear high costs and disaster risks.

Option 2: Renting Cloud and Computing Service
This solution involves using a third-party provider for cloud storage and computing, offering flexible and scalable resources.

Pros:

- Lower initial investment
- Scalability to meet growing business needs

Cons:

- Data privacy concerns with third-party providers
- Dependence on internet connectivity

Costs:
Monthly subscription costs based on usage.

Feasibility and Scalability:
Highly scalable solution that can be quickly implemented with minimal disruption.

Recommendation:
A viable option for businesses looking for flexibility and cost efficiency. However, data privacy concerns must be carefully managed.

Option 3: Hybrid Disaster Recovery Solution
This option combines on-premises infrastructure with cloud-based disaster recovery services to provide a balance between control and flexibility.

Pros:

- Enhances disaster recovery capabilities
- Flexible scalability with cloud resources

Cons:

- Complex to set up and manage
- Higher ongoing costs due to dual infrastructure

Costs:
Moderate upfront investment with ongoing costs for cloud services.

Feasibility and Scalability:
Suitable for businesses looking to balance data security with disaster recovery and scalability.

Recommendation:
Recommended for businesses that require both control and resilience in case of disasters, despite higher complexity and costs.

Option 4: Do Nothing (Maintain the Current Infrastructure)
This option involves making no changes and continuing with the current setup.

Pros:

- No additional costs or resource allocation
- Avoids disruption to current operations

Cons:

- Increased risk of data loss in case of failure
- Potential inability to scale with business growth

Costs:
No immediate investment but potential long-term losses due to system failure or inefficiencies.

Feasibility and Scalability:
Limited scalability and riskier in the long run.

Recommendation:
Not recommended, as it leaves the organization vulnerable to security threats and disaster scenarios without a recovery plan.

Cost/benefit analysis
These numbers are based on estimations from last year's audit and have been integrated by data engineers who have been tracking the price of the previous years. Disaster Recovery Costs and Cost Analysis Benefit. This approach has ensured that our projections are as close to accurate as possible. Our company's plan was to set out to chart a plan on how much a department for disaster recovery would cost. This timeframe plan covers highlighted capital expenditures and operational expenditures over a 5 year period. The projections allow us to calculate (YoY) Year-Over-Year. We focused the plan on being predictable so we could have the best (ROI) which is return of investment. Below we represent a breakdown of annual costs, covering key areas that range from electricity, employee salary, rental cost,heating etc.

5-year Timeframe for Disaster Recovery Cost

Project Development Cost	Initial Costs (US$)	Year 1 (US$)	Year 2 (US$)	Year 3 (US$)	Year 4 (US$)	Year 5 (US$)	Total (Combined)
Server Cost	19,000	2,850	2,850	2,850	2,850	2,850	33,250
Electricity Cost	6,000	5,700	5,700	5,700	5,700	5,700	34,500
Heating Cost	0	2,400	2,400	2,400	2,400	2,400	12,000
Cooling Cost	7,000	2,000	2,000	2,000	2,000	2,000	17,000
Employee Salary	0	685,700	685,700	685,700	685,700	685,700	3,428,500
Training Staff	8,000	6,000	6,000	6,000	6,000	6,000	38,000
Rental Cost: Office Space	12,000	28,500	28,500	28,500	28,500	28,500	154,500
Website Hosting	300	1,140	1,140	1,140	1,140	1,140	6000
Insurance	4,800	5,000	5,000	5,000	5,000	5,000	29,800

Gross Annual Costs	57,100	739,290	739,290	739,290	739,290	739,290	3,753,550

Below is the Cost Benefit Analysis table, which outlines and explains the expenditures of the time period of the last 5 years..
It's a very comprehensive look at breakdowns of the costs,initial investments,recurring costs, and benefits such as recurring expenses.
The analysis shows net benefit which shows the profitability over those 5 years in total which is 131,500 dollars.

Cost-Benefit Analysis Table

Category	Year 1 (US$)	Year 2 (US$)	Year 3 (US$)	Year 4 (US$)	Year 5 (US$)	Total Combined
Initial Start Costs	22,000					22,000
Recurring Costs (Annual)	20,000	20,000	20,000	20,000	20,000	100,000
Reduced Downtime	5,000	7,000	8,000	10,000	12,000	42,000
Employee Productivity	4,000	5,000	6,000	7,000	8,000	30,000
Customer Retention	2,500	3,000	4,000	5,000	6,000	20,500
Insurance Savings	1,000	1,000	1,000	1,000	1,000	5,000
Operational Efficiency	3,000	4,000	5,000	6,000	7,000	25,000
Total Benefits (5 Years)	60,000	80,000	100,000	120,000	140,000	500,000
Net Benefit (5 Years)	22,000	24,500	26,000	28,000	31,000	131,500
Total cost for each year	139,500	144,500	170,000	197,000	198,020	849,020

Impacts and Risks
There are several important impacts and risks a business must disclose, but we will be focusing on the most important ones. These can be split into four categories: operational improvements, market competitiveness, strategic growth and financial impacts. Risks on the other hand can be split into even more categories, like technical risks, security risks, project challenges, competitor risks, organizational risks and lastly financial risks.

Impacts:

Financial Impacts:

- Concrete benefits like cost-saving and increasing revenue
- Automating labour which decreases labour costs.
- New revenue streams through digital services and products
- Depending on digital services would make the company vulnerable to cyberattacks.

Operational Efficiency:

- Using AI to optimize the resource-usage for future projects and chatbots for customer support.
- Improving the dataflow between departments by integrating systems like ERP (Enterprise Resource Planning) and CRM (Customer Relationship Management).
- Inefficient integration or potential system failures could lead to system outages, which could lead to loss of sensitive business data.

Market and Customer Engagement:

- Analysing customer data to maintain a strong customer relationship by tailoring to meet the preferences and needs for each customer.
- Implementing loyalty programs to reward long standing customers to strengthen the relationship with them.
- Creating a user friendly and sophisticated web application builds credibility and trust towards the business.
- Developing, testing, and adapting to meet the criteria for a product based on feedback from the market.
- Excessive collecting of customer-data would raise concerns regarding customer privacy and could potentially lead to regulatory penalties if not regulated properly.

Technological Advancements:

- Automatizing labour decreases human errors and potentially saves work time.
- Transitioning from local servers to sky-based services gives the opportunity to either scale up or down resources as needed.
- Developing, testing, and adapting to meet the criteria for a product based on feedback from the market.
- Using AI to detect and prevent future cyberattacks.
- AI-based cyber defense-tools may generate false positives, or fail to detect advanced security-threats, creating a false sense of security.

Organizational Development:

- Refreshing the employee's skills by doing routine workshops.
- Using AI for data-analysis to help make smarter decisions strategically.
- Implement a management framework like Scrum to handle and adapt to complex projects.
- Routine workshops can be expensive and time consuming, which would reduce the productivity of the company.

Risks:

Technical Risks:

- Critical components like servers and network devices can malfunction.
- Major issues like network outages will stop the operation.
- System components get outdated quickly and buying new equipment is costly.
- Migrating from older systems could lead to issues, and in worst case loss of data.
- Can manage these risks by having regular maintenance and monitoring. By monitoring the system regularly we can detect system errors early.

Security Concerns:

- Cybercriminals could gain access to sensitive data through system flaws.
- Employees with access to sensitive data could be exposed to social engineering attacks, which could potentially put the entire organization at risk.
- Unencrypted data could get swept up by malicious actors in storage or while transferring it.
- By having controlled access we can enforce policies and multi-factor authentication for no breach.

Project-specific challenges:

- Project demands may change over time, which makes it harder to adapt to the adjustments in time, budget, and resource usage.
- Projects tied to specific geographical locations would face challenges while scaling, making them less viable for reaching expanding markets.
- Compatibility issues may arise when integrating new systems with existing infrastructure.
- These risks can be mitigated by adopting an agile method. This way we can ensure improvements along the way.

Competitor Risks:

- Competitors may try to control the market share by lowering prices significantly.
- Competitors may introduce more advanced and profitable solutions, which makes lesser solutions invaluable.
- Competitors may have a legacy that attracts customers, even if their technology is inferior.
- By monitoring the industry trends, we can be active in searching for coming market shifts, this way we can adapt quickly.

Organizational Risks:

- Departments may only focus on their specific goals, instead of cooperating with other departments towards an organizational objective.
- Over-relying on key employees for critical tasks may lead to issues in the future if these individuals were to either become ill or leave the company.
- Failing to identify potential risks during project planning may result in unexpected challenges and issues, which lowers the chances of the project being a success.
- By documenting progress we can reduce the dependency of individuals.

Financial Risks:

- The budget may fail due to underestimating costs, with hidden expenses and unexpected challenges not considered.
- Cash flow issues may arise if project payments are delayed, or if expenses are higher than predicted.
- Investments in technology may become invaluable due to swift advancements or changes within the industry.
- By being aware of certain risks like these, we can set aside a portion of the budget.

Risks and Mitigation

Risks	Mitigation
Technical Risks: Hardware failure, network issues	Redundant systems and regular maintenance, cloud-based backups, network monitoring.
Security Risks: Cyberattacks, social engineering	Multi-factor authentication, protocols, staff training. intrusion detection systems, regular pentesting.
Project Risks: Scope creep, integration issues	Agile project management, change management process, regular stakeholder reviews.
Organizational Risks: Lack of leadership continuity, high employee turnover	Strong internal communication, define clear roles, implement succession planning and leadership.
Financial Risks: Budget overruns, cash flow issues	Conduct regular financial audits, prioritize scalable solutions, build an emergency reserve, diversify funding.

Conclusion and recommendation

We recommend Option 3, the Hybrid Disaster Recovery solution. This solution leverages both on-premises infrastructure for enhanced data security and control, while utilizing cloud based services for scalability and rapid recovery capabilities. This approach provides flexibility and scalability for our business in case of future changes.

The hybrid approach also offers better cost-effectiveness compared to a fully cloud-based solution while maintaining robust security measures. Our cost-benefit analysis indicates that this solution will provide the best return on investment over the five-year period, with projected savings in both operational costs and downtime reduction.

Reference:

LA Times. (2017, August 17). *Cyberattack cost Maersk up to $300 million and disrupted operations for 2 weeks*. Los Angeles Times. https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html

IBM. (2024). *Cost of a data breach report 2024*. Hentet fra: Cost of a Data Breach Report 2024

Cadle, J. & Yeates, D. (2008). *Project management for information systems (5th ed).* Pearson Education Limited 2008

Assignment 3: Choosing a Development Lifecycle

Why spiral model?

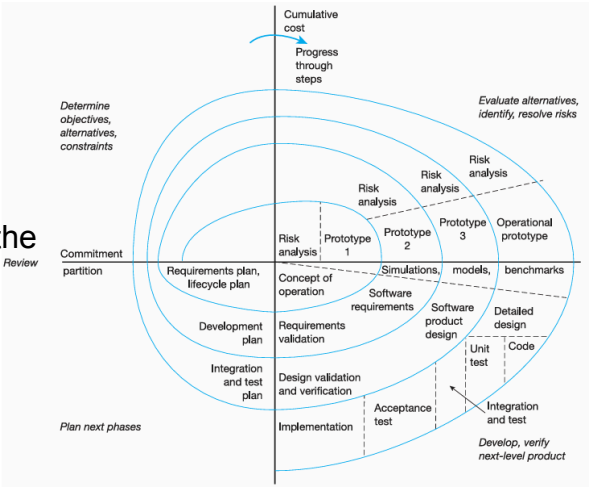
We have determined that the Spiral Model is the most suitable for our approach for the development and implementation of our disaster recovery and continuity program. This is based on the models ability to address high uncertainty, accommodating the evolving requirements and still maintain a strong focus on risk management. Reasons we choose the spiral model is:

1. *Focus on risk analysis*
   At each phase there's focus on risk analysis, by having this built in it just shows that it's the most strategic thing to do. Fortunately, the entire top-right quadrant of the spiral model focuses on this. Great approach for disaster recovery, by identifying the threats before implementation we can prevent further destruction down the line.

2. *Improvements*
   The spiral model is set up by a couple of cycles. By each cycle we can improve our security protocols and address new threats. The bottom right corner is especially a good example of that, since there's focus on validating and checking up on the software. This way we can stay ahead of the curve and push out updates to address our goals.

   Each cycle in the Spiral Model follows a structured approach which lets us identify objectives, assess different risks, develop prototypes and validate the different solutions implemented. This process ensures that the system can remain adaptive to evolving cyber threats and other regulatory changes such as refining staff training protocols.

3. *Leaders and stakeholders*
   Regular review in each cycle lets leaders, the IT team, stakeholders provide inputs and ability to validate different progress and prototype to ensure that it aligns with the business goals and expectations.



Bohem's spiral model
(Cadle, J. & Yeates, D. 2008. s.75)

The spiral model vs agile
Agile model is a more modern and iterative approach that breaks the project into small increments called sprints,which last anywhere between 2-4 weeks. Each sprint involves planning, development,testing and review.

We chose the **Spiral Lifecycle Model** because it suited our earlier risk assessment model. Considering the fact that our project involves scenarios such as cyberattacks and natural disasters, the Spiral Model's risk analysis phase was the ideal way to ensure that potential risks are assessed and identified early in each iteration. This aligns perfectly with our project's mission plan.
The Spiral model uses iterative development in each cycle. Each cycle or spiral consists of four phases:

- Planning
- Risk Analysis
- Engineering
- Evaluation

The spiral model vs waterfall

Risk management, the spiral model is much better for risk management compared to the waterfall model. Our project involves disaster recovery and IT security, where identifying risks as early as possible is crucial. The waterfall model only assesses risks at the beginning, whereas the spiral model allows continuous risk analysis and mitigation throughout the development process.

Flexibility, the spiral model is highly flexible, allowing changes throughout the project. Since cyber threats evolve fast, the spiral model ensures that we can adapt security measures as new threats emerge. In contrast, the waterfall model struggles with changes, as each phase must be completed before moving to the next.

Testing and adaptability, disaster recovery planning requires a lot of testing, which the spiral model accommodates well. The waterfall's step by step process makes it difficult to adjust security protocols once a phase is completed.

For a disaster recovery project, the spiral model is by far the better choice compared to waterfall. Its strong focus on risk management and iterative development makes it ideal for evolving security challenges. Meanwhile, the waterfall model is better suited for projects with clear requirements and low risk.

MEMO
To: Team members & Stakeholders
From: Chief Executive Officer & Chief Operating Officer
Date: 30.01.2025
Subject: Decision on Development Lifecycle - Adoption of the Spiral Model

After thorough analysis, we have determined that the Spiral Model is the most suitable development lifecycle for our disaster recovery and continuity program. This decision is based on the model´s ability to handle high uncertainty, accommodate evolving requirements, and maintain a strong focus on risk management.

Key Reasons for Choosing the Spiral Model

1. *Risk Management*

- Risk analysis is a key component of the spiral model at every phase, ensuring proactive threat identification.
- The models give us the opportunity to assess vulnerabilities before implementation, preventing potential disruptions.

2. *Continuous Improvement*

- The iterative nature of the Spiral Model enables ongoing enhancements to security protocols.
- Each cycle includes validation and testing, allowing us to always stay ahead of evolving threats.

3. *Adaptability for Hybrid Infrastructure*

- Our project involves on-premises and cloud-based solutions, requiring flexibility in testing across multiple locations.
- The Spiral Model allows controlled testing and adjustments without major disruptions to infrastructure.

4. *Comparison to Waterfall Model*

- Unlike the Waterfall model, which only assesses risk in the initial phase, the Spiral model provides continuous risk analysis.
- Cybersecurity threats evolve rapidly, and the flexibility of the Spiral model ensures we can adapt as new risks emerge.
- The iterative approach facilitates ongoing testing and adaptability, which is crucial for disaster recovery planning.

Conclusion
Given the need for strong risk management, adaptability, and continuous improvement, the Spiral Model is the optimal choice for our project. Its iterative nature aligns with the dynamic nature of cybersecurity threats, allowing us to enhance security measures proactively. While the Waterfall Model may be effective for projects with stable requirements, our disaster recovery program demands a more agile and risk aware approach.

If you have any further questions or need more indepth clarification, please feel free to reach out.

Best regards,
Ola Nordmann, Chief Executive Officer (CEO)

Reference:

Cadle, J. & Yeates, D. (2008). *Project management for information systems (5th ed).* Pearson Education Limited 2008

Assignment 4: Product backlog

Sprint 1:
User stories with acceptance criteria
Below you can read about user stories that in depth describes how our project of disaster recovery and business continuity is critically important when it comes to system monitoring, secure backup systems, incident response and downtime minimizing.

System Monitoring	Secure Backup system	Incident Response Workflow	Minimizing Downtime
Interface	Backup scheduling	Categorizing of incidents	Real-time monitoring
Hardware tracking	Storing	Alerts	Automated rollback
Alert system	Encrytion	Automated response	RTO

Real-Time System Monitoring (High priority)
As a System Administrator,
I want to monitor each critical systems in real time,
so that I can detect and resolve issues before they can escalate to bigger problems and disasters.

Acceptance Criteria:
- An interface with different tools that monitors critical systems in real time.
- Tracking hardware usage, is there anything that is operating abnormally?. (CPU, memory, disk, network)
- Implement an alert system that is configured to notify the IT team abnormal and metrics exceed predefined thresholds.

Multi-Layered Incident Response Workflow
As an Incident Response Coordinator,
I want to implement a multi-layered incident response workflow that automates containment and mitigation procedures,
so that the company can minimize downtime and data exposure during cyberattacks.

Acceptance Criteria:

- Incident response workflow must classify incidents into categories (e.g., phishing, malware, data breach, DDoS attack).
- Automated playbooks should trigger predefined responses for each incident type.
- Communication protocols should include immediate alerts to key stakeholders and affected departments.
- Incident logs should be maintained for forensic analysis and post-incident review.
- Workflow should integrate with the AI-powered threat detection system for real-time intelligence sharing.

Secure backup system (High priority)
As a system administrator,
I want to include an automated backup system that stores data in several locations,
so that data loss is kept to a minimum in case of a disaster.

Acceptance criteria:

- Automatic backup scheduling
    - Backup needs to be automatically with a set time interval.
    - Infrastructure systems: every hour.
    - Business data: every 24 hours.
- If the backup was to fail, the system must retry a backup once more before sending out an alert.
- On premises + cloud storage
    - backups have to be stored in separate locations since our recommendations are based on on-premises and cloud based storages.

Minimizing Downtime (Low priority)
As an IT Security Manager,
I want to implement an automated system that reduces downtime during incidents,
so that business operations can continue with minimal disruption.

Acceptance criteria:

- Run regular incident response drills to test recovery plans.
- Limit downtime with a defined Recovery Time Objective (RTO).
- Maintain backup systems in multiple locations for redundancy.
- Enable automated rollback to restore stable versions if needed.

- Generate a report after each downtime event to analyze and improve recovery.
- Implement a real-time monitoring with alerts to detect and respond fast.

Sprint 2:
Improve system monitoring with AI (High priority)
Proactive monitoring is critical for identifying potential failures early, ensuring the reliability and stability in our IT systems. It helps prevent minor issues from escalating into major disasters. By continuously tracking hardware usage and system performance we can:

- *Improve response time:*
    - By implementing a real time monitoring and alert system, the IT team can get notified and respond quickly to anomalies, minimizing the impact on our operations.
- *Prevent downtime:*
    - As mentioned in improved response time, by detecting issues before they escalate to major disasters helps prevent downtime. The IT team is alerted and fixes the issues.
- *Enhance risk management:*
    - Monitoring aligns with the Spiral Models focus on risk analysis by providing a continuous visibility into critical systems health.
    - Allows us to identify and mitigate risks before they escalate, ensuring our disaster recovery program remains robust and effective.
    - AI-driven anomaly detection must analyze network traffic, login attempts, and system behavior in real time.
    - Threat detection systems should automatically generate alerts and classify threats based on severity levels.
    - Must integrate with SIEM (Security Information and Event Management) solutions for centralized security monitoring.
    - Automated response mechanisms should be implemented for critical threats, such as blocking IPs or isolating affected systems.
    - System should provide weekly reports with security insights and incident analysis.

Secure backup system (High priority)
Acceptance Criteria
- Automatic Backup Scheduling
- Backup must be executed automatically at predefined time intervals:
    - Infrastructure systems: Every hour.
    - Business data: Every 24 hours.

- if a scheduled backup fails, the system must:
  -Retry the backup once before triggering an alert.
  -Send notifications to the system administrator if the second attempt also fails.

- On-Premises + Cloud Storage
- Backup must be stored in separate locations to ensure redundancy
- The backup system must support both on-premises and cloud-based storage solutions.
- Backups should be encrypted before being transmitted to ensure security.

- Compliance with the 3-2-1 Backup Rule
- Maintain at least three copies of all critical data.
- Store copies in at least two different types of storage media (e.g., local disk, cloud, or network-attached storage).
- Keep at least one copy off-site (e.g., cloud storage or a remote data center) to protect against local disasters.

Additional Considerations for Future Enhancements
- Implement end-to-end encryption (AES-256*) for secure data storage.
- Automate backup integrity verification through checksum validation.
- Introduce immutable backups to protect against ransomware attacks.
- Provide real-time monitoring and alerting for failed or delayed backups.

Improve the automated system to minimize downtime (Low priority)
Develop and improve an automatic system that can efficiently handle system errors and downtime to ensure business operations continue with no disruption. This will build upon the systems implemented in sprint 1, and give a more advanced monitoring and automation to enable faster recovery.

- Run regular incident response drills to test recovery plans
  - Plan and run incident response drills every few months to simulate attacks.
  - Make sure the IT team knows the recovery steps and can respond fast within the RTO.
- Limit downtime with a defined Recovery Time Objective (RTO).
  - Set clear RTOs for critical systems to reduce downtime, automate recovery to meet these goals fast.
  - Minimize downtime and ensure systems are restored within the set RTO.
- Maintain backup systems in multiple locations for redundancy.

    - Set up backups in the cloud and test them regularly to ensure they remain up to date.
    - This will allow for quick restoration of data and systems when needed.
- Enable automated rollback to restore stable versions if needed.
    - Set up an automated rollback process that can restore stable versions of systems and applications if something goes wrong.
    - This will reduce the need for manual fixes and speed up the recovery process.
- Generate a report after each downtime event to analyze and improve recovery.
    - After each downtime, create a report that includes the cause, time taken to recover and issues.
    - Use the report to find weaknesses in the recovery process and improve it for the future.
- Implement a real-time monitoring with alerts to detect and respond fast
    - Set up a real-time monitoring to track the system performance and alert about critical issues.
    - This will ensure fast responses to prevent minor issues from growing, keeping business operations running smoothly.

Planned Product Backlog Items (PBIs)

1. **Real-Time System monitoring (High Priority)**
   Objective: Implement comprehensive monitoring of critical systems to be able to detect and resolve issues proactively.
   Key Features:
   - Dashboard interface displaying real-time system metrics
   - Hardware performance tracking (CPU, memory, disk,network)
   - Threshold-based alert system for anomalies

   Outcome: Early detection of issues to prevent escalation into major failures. Supports Iron Triangle Scope by focusing on core disaster recovery needs.

2. **Multi-layered Incident Response Workflow (High Priority)**
   Objective: Automate incident containment and mitigation to minimize downtime during cyberattacks.
   Key Features:
   - Incident categorization (phishing, malware, DDoS, etc.)
   - Automated playbooks for predefined responses)
   - Alert system for stakeholders and forensic logging

   Outcome:Faster, standardized responses to security incidents.

3. **Secure Backup System (High Priority)**
   Objective: Ensure data redundancy and quick recovery through automated backups.
   Key Features:
   - Schedules backups (hourly for infrastructure, daily for business data)
   - On-premise + cloud storage with added encryption
   - Compliance with 3-2-1- backup rule (3 copies,2 media types, 1 off-site)

   Outcome: Minimized data loss during disasters.

4. **AI-Powered Monitoring Enhancement (Sprint 2 - High Priority)**
   Objective: Integrate AI for proactive threat detection and system health analysis.
   Key Features:
   - Anomaly detection in network traffic and system behavior
   - Automated alerts and threat classification
   - Integration with SIEM tools

   Outcome: Improved risk management and faster threat response.

5. **Downtime Minimization (Low Priority)**
   Objective: Reduce operational disruption through automated recovery processes.
   Key Features:
   - Regular incident response drills
   - Defined Recovery Time Objectives (RTOs)
   - Automated rollback and multi-location backup

   Outcome: Business continuity during system failures.

References

Acronis. (2023, 23.september) Auto backup - all you need to know. https://www.acronis.com/en-us/blog/posts/auto-backup/#Nkhj951mkW

Assignment 5: Project initiation

Project definition and scope

Background:
Businesses face increasing risks of cyber threats, operational disruptions and other security risks on a daily basis. This project aims to implement a robust Disaster recovery and Business Continuity plan, which is essential to ensuring resilience.

We have taken lessons and learned from past cyber incidents, such as the 2017 MAERSK cyberattack, which highlighted the critical need for disaster recovery planning. This project aims to develop and implement a hybrid infrastructure solution which integrates an on-premises and cloud-based system to minimize downtime and also secures the business operations.

Scope of the project

- Implementation of option 3 as mentioned earlier: a hybrid disaster recovery solution which involves an on-premises and cloud-based system.
- The project will focus on implementing automation and scheduled monitoring rather than having a response team on the clock 24/7.
- Development of a real-time monitoring and AI integrated alert system
- Establishment of automated backup scheduling for infrastructure and business data.
- Regular staff training and disaster recovery drills.

Out-of-scope
(Exclusions)

- 24/7 Dedicated IT Staff
    - Having a dedicated response team on the clock 24/7 for live monitoring and support will not be implemented, but instead rely on AI-monitoring tools.
- Full on-premises or cloud-only infrastructure
    - A full on premises or cloud infrastructure will not be implemented due to budget restraints, as well as scalability.
- Legacy system migration
    - We will not include migrations of legacy applications or outdated systems unless critical for disaster recovery.

Constraints and Assumptions

- *Constraints:*
    - The project must be executed within the allocated budget and timeline listed in the business case summary, which is 12-15 months.
    - Regulatory Compliance: The project must adhere to industry standards such as ISO 22301:2019 (Security and resilience - Business continuity management systems), General Data Protection Regulation (GDPR) and NIST cybersecurity frameworks. (ISO, 2019 and GDPR, n.d)
- *Assumptions:*
    - Cloud services availability: The project assumes that chosen cloudplatform will have high availability and reliability. (AWS, Azure, Google cloud)
    - Stakeholders support: The project assumes that stakeholders will continue to back the initiative with funding and policy support.

Interfaces

- *Cloud service integrations*
    - AWS, Microsoft Azure or Google Cloud for secure back and data recovery
- *Security and monitoring*
    - SIEM solutions for our real time threat detection and incident response.

Project Approach / Milestones

Project Implementation Approach

The project will be executed in a structured and phased manner to ensure that the disaster recovery, business continuity, and infrastructure implementation processes are successfully carried out. The implementation follows industry best practices and established frameworks, such as PRINCE2 and ISO 22301 for Business Continuity Management, as well as the OWASP Testing Guide for security assessments. The Spiral Model has been chosen as the development lifecycle due to its iterative approach, focus on risk management, and adaptability to evolving requirements.

Purpose of the Project Initiation Document (PID)

The purpose of the PID is to define the project and provide a foundation for its management and assessment of its success. The PID serves three primary purposes:

- Ensuring that the project has a sound basis before making major commitments.

- Acting as a reference for project board and project manager assessments.
- Providing a single source of project-related information for new team members.

The PID remains a living document, updated as necessary throughout the project lifecycle to reflect the latest plans, controls, and current status.

Processes and Procedures

To accomplish the objectives of the project, the following processes and procedures will be implemented:

1. *Project Definition and Scope*
    - Define project objectives and desired outcomes.
    - Identify project constraints, assumptions, and exclusions.
    - Establish stakeholder and user requirements.

2. *Risk Assessment and Planning*
    - Identify critical systems and potential threats.
    - Conduct a SWOT analysis to understand strengths, weaknesses, opportunities, and threats.
    - Define risk mitigation strategies and establish security protocols.

3. *Infrastructure Implementation*
    - Set up a hybrid infrastructure combining on-premises and cloud-based solutions.
    - Establish backup and redundancy planning to minimize downtime.
    - Implement a multi-layered incident response workflow.

4. *Project Management Team Structure and Roles*
    - Define the roles of the project management team.
    - Establish responsibilities and reporting structures.

5. *Quality Management Approach*
    - Apply quality standards and techniques for disaster recovery.
    - Conduct regular audits and assessments to ensure compliance.

6. *Security Enhancements and Monitoring*
    - Deploy AI-driven real-time system monitoring.
    - Implement multi-factor authentication and role-based access controls.
    - Conduct regular security audits and penetration testing.
7. *Change Control and Risk Management*
    - Establish a structured approach to change management.

    - Maintain a risk register and apply risk mitigation strategies.

8. *Training and Staff Readiness*
    - Conduct regular disaster recovery drills.
    - Train employees on threat detection and response strategies.
    - Develop a structured incident response plan and testing methodology.

9. *Communication Management Approach*
    - Define key stakeholders and the communication strategy.
    - Establish reporting mechanisms and frequency.

10. *Testing and Validation*
    - Perform continuous risk analysis and iterative improvements using the Spiral Model.
    - Validate system integrity and performance through simulations and stress testing.
    - Document findings and refine protocols based on test outcomes.

Key Milestones

To ensure project transparency and structured execution, the following milestones have been established:

Phase 1: Project Initiation (Month 1-3)

- Define project scope and objectives.
- Conduct initial risk assessment.
- Establish key project roles and responsibilities.
- Develop project plan and framework selection.
- Create an initial version of the PID.

Phase 2: Infrastructure Implementation (Month 4-7)

- Set up core infrastructure components (on-premises and cloud-based solutions).
- Configure secure backup systems with redundancy measures.
- Establish access control measures and cybersecurity protocols.
- Apply PRINCE2 principles to ensure process control.

Phase 3: Security Enhancements and Training (Month 8-10)

- Deploy real-time monitoring tools and AI-driven threat detection.
- Implement automated incident response workflows.
- Conduct employee training sessions and awareness programs.

Phase 4: Testing and Risk Mitigation (Month 11-12)

- Perform penetration testing and vulnerability assessments.
- Validate disaster recovery protocols through controlled drills.
- Analyze test results and refine security measures.

Phase 5: Final Deployment and Review (Month 13-15)

- Execute final validation of disaster recovery and business continuity strategies.
- Conduct final stakeholder review and obtain approval.
- Deploy a full-scale operational plan and establish ongoing monitoring processes.

Project Controls and Tailoring of PRINCE2

- Management stage boundaries and reporting mechanisms will be applied.
- Monitoring and reporting processes will ensure compliance with project objectives.
- PRINCE2 will be tailored to fit the needs of this specific project, ensuring adaptability.

Communication and Documentation

The project team will maintain clear and consistent communication with all stakeholders through:

- Monthly progress reports detailing milestone achievements and risks.
- Documentation of test results, security assessments, and improvement plans.
- Regular review meetings with leadership and key project stakeholders.

This structured approach ensures that the disaster recovery and business continuity plan is successfully implemented while minimizing disruptions and optimizing security protocols.

Business case summary

Introduction and background

On a day to day basis, businesses are facing a constant threat of cyberattacks and other critical disruptions that can impact the businesses operations severely. These types of disruptions can range from, hardware failures, natural disasters, war, cyber threats and even human errors. In 2017, MAERSK fell victim to a devastating cyberattack that cost them approximately $300 million in damages in only two weeks (LA Times, 2017). The attack disrupted their global operations for weeks, impacting numerous companies that relied on Maersk for shipping their products. This highlights the importance of having a robust disaster recovery continuity system. Therefore, we propose establishing a dedicated department for disaster recovery and business continuity management.

Management summary

This document presents a business case for implementing a disaster recovery and business continuity plan, which is supported by modern infrastructure. The goal is to ensure the organization can withstand any cyberattacks and technical disruptions, minimizing downtime and financial impact.

What:

- This project involves implementing and designing a robust disaster recovery and business continuity plan. This includes developing infrastructure, establishing backup systems, and ensuring critical operations can continue during and after incidents with strict protocols. By learning from incidents like the MAERSK cyberattack, we can better prepare ourselves to handle similar incidents or and other challenges.

Why:

- There are several key benefits of implementing a disaster recovery and business continuity solution:
    - Faster recovery: Reducing recovery time from cyberattacks or technical failures minimizes the impact on company operations.
    - Financial protection: Rapid recovery prevents significant financial losses, as demonstrated by the MAERSK incident.
    - Staff readiness: Training staff to handle incidents improves overall company response time.
    - Trust and reputation: A robust and solid strategy enhances the company's reputation among customers, partners, and investors.

Cost:

- The initial cost will be high, covering infrastructure setup, security enhancements, staff training, and a department for continuous monitoring. Although these setup costs are significant, the long-term benefits and financial savings from reduced downtimes, increased operational efficiency, and lower risk of data loss can outweigh the upfront expenses.

Timeline:

- Estimated time of getting the infrastructure and system up and running is expected to take 12-15 months.

Problem
This project aims to reduce the frequency of technical failures, cyberattacks and other disruptions that may arise to make sure that the business and infrastructure is secure. Based on this we have come up with four possible ways of ensuring this.

- *Option 1: on-premises infrastructure*
  While effective this can be very demanding in the longer run, it requires high capital expenditure and a full department that works around the clock.

- *Option 2: Cloud infrastructure*
  By choosing this option, all systems, data, storage and much more gets migrated to a cloud platform, like google cloud or Amazon web services. This would result in a lower disaster recovery time. This will also bring problems like data security, since there would be a huge reliance on using these cloud services and risks of breaches.

- *Option 3: On-premises and cloud based (recommended)*
  This is the most reliable way when it comes to cost. By having on-premises we can focus on disaster recovery, and situational training. While with cloud-based infrastructure, we can guarantee faster recovery and greater focus on security by encrypting data, implementing multi-factor authentication and regular vulnerability assessments.

- *Do Nothing (Maintain the Current Infrastructure)*
  This option involves making no changes and continuing operations as normal with the current setup. No additional cost or resources are needed and will avoid disrupting any current operations.

Based on these options, we highly recommend going with Option 3,The on-premises and cloud based infrastructure implementation option offers a great amount of strength by combining these two infrastructures together. Mainly by ensuring a quick

recovery and stronger security. This investment may seem like a lot, but a key factor here is that this is a long term investment that definitely can yield positive results.

Description of problem or opportunity
By not having a dedicated department for disaster recovery and basic It security the organization is at great risk. Cyber threats are rapidly growing and becoming more sophisticated and frequent. The result of a cyberattack could lead to major financial losses, data breaches and harm to the company's reputation.

Additionally, nowadays it is almost mandatory to have proper IT security measures in place to meet industry standards. Regulations like ISO 22301 emphasize the need for disaster recovery and business continuity. Failure to comply with these standards could result in fines or penalties.

Improved security and rapid response:
As mentioned earlier in the SWOT analysis under strengths, a dedicated disaster recovery team would improve security and reduce downtime during cyberattacks. In today's landscape of growing cyber threats, being able to respond fast is crucial for business continuity.

Data Redundancy and risk reduction:
Setting up multiple data centers will help reduce the risk of permanent data loss. This will ensure that critical data remains secure and is accessible during incidents.

Trust and reputation:
Implementing a good disaster recovery department can result in better reputation and build trust with the customers and stakeholders.

Long-Term investment:
While the initial investment may seem like a lot, implementing a disaster recovery department would be of extreme value. It will reduce financial losses in the future by ensuring a faster recovery from an incident. According to the IBM Cost of a Data Breach Report 2024, the global average cost of a data breach in 2024 was $4.88 million (IBM, 2024, p. 8). This shows why taking action early is important.

Options available and considered
Option 1 provides tighter security with on-premises hardware but comes with higher costs and risks of physical disasters. Option 2 offers a cost-effective cloud solution with scalable resources but has potential data privacy concerns. Option 3 combines the strengths of both on-premises and cloud solutions for enhanced disaster recovery but involves higher complexity. Option 4 considers doing nothing, maintaining the current infrastructure without additional investment.

Option 1: Physical Hardware On-Site
This option involves investing in physical hardware that is stored and maintained on-site, ensuring tighter control over data and security protocols.

Pros:

- Higher security due to on-site hardware control
- Reduced risk of third-party breaches

Cons:

- High upfront and maintenance costs
- Increased vulnerability to natural disasters (flood, fire, etc.)

Costs:
Significant initial investment for hardware and ongoing maintenance expenses.

Feasibility and Scalability:
Suitable for organizations prioritizing data control and security. Limited scalability due to physical infrastructure.

Recommendation:
Not recommended unless the organization has a critical need for on-premises security and is willing to bear high costs and disaster risks.

Option 2: Renting Cloud and Computing Service
This solution involves using a third-party provider for cloud storage and computing, offering flexible and scalable resources.

Pros:

- Lower initial investment
- Scalability to meet growing business needs

Cons:

- Data privacy concerns with third-party providers
- Dependence on internet connectivity

Costs:
Monthly subscription costs based on usage.

Feasibility and Scalability:
Highly scalable solution that can be quickly implemented with minimal disruption.

Recommendation:
A viable option for businesses looking for flexibility and cost efficiency. However, data privacy concerns must be carefully managed.

Option 3: Hybrid Disaster Recovery Solution
This option combines on-premises infrastructure with cloud-based disaster recovery services to provide a balance between control and flexibility.

Pros:

- Enhances disaster recovery capabilities
- Flexible scalability with cloud resources

Cons:

- Complex to set up and manage
- Higher ongoing costs due to dual infrastructure

Costs:
Moderate upfront investment with ongoing costs for cloud services.

Feasibility and Scalability:
Suitable for businesses looking to balance data security with disaster recovery and scalability.

Recommendation:
Recommended for businesses that require both control and resilience in case of disasters, despite higher complexity and costs.

Option 4: Do Nothing (Maintain the Current Infrastructure)
This option involves making no changes and continuing with the current setup.

Pros:

- No additional costs or resource allocation
- Avoids disruption to current operations

Cons:

- Increased risk of data loss in case of failure
- Potential inability to scale with business growth

Costs:
No immediate investment but potential long-term losses due to system failure or inefficiencies.

Feasibility and Scalability:
Limited scalability and riskier in the long run.

Recommendation:
Not recommended, as it leaves the organization vulnerable to security threats and disaster scenarios without a recovery plan.

Cost/benefit analysis
These numbers are based on estimations from last year's audit and have been integrated by data engineers who have been tracking the price of the previous years. Disaster Recovery Costs and Cost Analysis Benefit. This approach has ensured that our projections are as close to accurate as possible. Our company's plan was to set out to chart a plan on how much a department for disaster recovery would cost. This timeframe plan covers highlighted capital expenditures and operational expenditures over a 5 year period. The projections allow us to calculate (YoY) Year-Over-Year. We focused the plan on being predictable so we could have the best (ROI) which is

return of investment. Below we represent a breakdown of annual costs, covering key areas that range from electricity, employee salary, rental cost,heating etc.

5-year Timeframe for Disaster Recovery Cost

Project Development Cost	Initial Costs (US$)	Year 1 (US$)	Year 2 (US$)	Year 3 (US$)	Year 4 (US$)	Year 5 (US$)	Total (Combined)
Server Cost	19,000	2,850	2,850	2,850	2,850	2,850	33,250
Electricity Cost	6,000	5,700	5,700	5,700	5,700	5,700	34,500
Heating Cost	0	2,400	2,400	2,400	2,400	2,400	12,000
Cooling Cost	7,000	2,000	2,000	2,000	2,000	2,000	17,000
Employee Salary	0	685,700	685,700	685,700	685,700	685,700	3,428,500
Training Staff	8,000	6,000	6,000	6,000	6,000	6,000	38,000
Rental Cost: Office Space	12,000	28,500	28,500	28,500	28,500	28,500	154,500
Website Hosting	300	1,140	1,140	1,140	1,140	1,140	6000
Insurance	4,800	5,000	5,000	5,000	5,000	5,000	29,800
Gross Annual Costs	57,100	739,290	739,290	739,290	739,290	739,290	3,753,550

Below is the Cost Benefit Analysis table, which outlines and explains the expenditures of the time period of the last 5 years..
It’s a very comprehensive look at breakdowns of the costs,initial investments,recurring costs, and benefits such as recurring expenses.
The analysis shows net benefit which shows the profitability over those 5 years in total which is 131,500 dollars.

Cost-Benefit Analysis Table

Category	Year 1 (US$)	Year 2 (US$)	Year 3 (US$)	Year 4 (US$)	Year 5 (US$)	Total Combined
Initial Start Costs	22,000					22,000
Recurring Costs (Annual)	20,000	20,000	20,000	20,000	20,000	100,000
Reduced Downtime	5,000	7,000	8,000	10,000	12,000	42,000
Employee Productivity	4,000	5,000	6,000	7,000	8,000	30,000
Customer Retention	2,500	3,000	4,000	5,000	6,000	20,500
Insurance Savings	1,000	1,000	1,000	1,000	1,000	5,000
Operational Efficiency	3,000	4,000	5,000	6,000	7,000	25,000
Total Benefits (5 Years)	60,000	80,000	100,000	120,000	140,000	500,000
Net Benefit (5 Years)	22,000	24,500	26,000	28,000	31,000	131,500
Total cost for each year	139,500	144,500	170,000	197,000	198,020	849,020

Impacts and Risks

There are several important impacts and risks a business must disclose, but we will be focusing on the most important ones. These can be split into four categories: operational improvements, market competitiveness, strategic growth and financial impacts. Risks on the other hand can be split into even more categories, like technical risks, security risks, project challenges, competitor risks, organizational risks and lastly financial risks.

Impacts:

Financial Impacts:

- Concrete benefits like cost-saving and increasing revenue
- Automating labour which decreases labour costs.
- New revenue streams through digital services and products
- Depending on digital services would make the company vulnerable to cyberattacks.

Operational Efficiency:

- Using AI to optimize the resource-usage for future projects and chatbots for customer support.
- Improving the dataflow between departments by integrating systems like ERP (Enterprise Resource Planning) and CRM (Customer Relationship Management).
- Inefficient integration or potential system failures could lead to system outages, which could lead to loss of sensitive business data.

Market and Customer Engagement:

- Analysing customer data to maintain a strong customer relationship by tailoring to meet the preferences and needs for each customer.
- Implementing loyalty programs to reward long standing customers to strengthen the relationship with them.
- Creating a user friendly and sophisticated web application builds credibility and trust towards the business.
- Developing, testing, and adapting to meet the criteria for a product based on feedback from the market.
- Excessive collecting of customer-data would raise concerns regarding customer privacy and could potentially lead to regulatory penalties if not regulated properly.

Technological Advancements:

- Automatizing labour decreases human errors and potentially saves work time.
- Transitioning from local servers to sky-based services gives the opportunity to either scale up or down resources as needed.
- Developing, testing, and adapting to meet the criteria for a product based on feedback from the market.
- Using AI to detect and prevent future cyberattacks.
- AI-based cyber defense-tools may generate false positives, or fail to detect advanced security-threats, creating a false sense of security.

Organizational Development:

- Refreshing the employee's skills by doing routine workshops.
- Using AI for data-analysis to help make smarter decisions strategically.
- Implement a management framework like Scrum to handle and adapt to complex projects.
- Routine workshops can be expensive and time consuming, which would reduce the productivity of the company.

Risks:

Technical Risks:

- Critical components like servers and network devices can malfunction.
- Major issues like network outages will stop the operation.
- System components get outdated quickly and buying new equipment is costly.
- Migrating from older systems could lead to issues, and in worst case loss of data.
- Can manage these risks by having regular maintenance and monitoring. By monitoring the system regularly we can detect system errors early.

Security Concerns:

- Cybercriminals could gain access to sensitive data through system flaws.
- Employees with access to sensitive data could be exposed to social engineering attacks, which could potentially put the entire organization at risk.
- Unencrypted data could get swept up by malicious actors in storage or while transferring it.
- By having controlled access we can enforce policies and multi-factor authentication for no breach.

Project-specific challenges:

- Project demands may change over time, which makes it harder to adapt to the adjustments in time, budget, and resource usage.
- Projects tied to specific geographical locations would face challenges while scaling, making them less viable for reaching expanding markets.
- Compatibility issues may arise when integrating new systems with existing infrastructure.
- These risks can be mitigated by adopting an agile method. This way we can ensure improvements along the way.

Competitor Risks:

- Competitors may try to control the market share by lowering prices significantly.
- Competitors may introduce more advanced and profitable solutions, which makes lesser solutions invaluable.
- Competitors may have a legacy that attracts customers, even if their technology is inferior.
- By monitoring the industry trends, we can be active in searching for coming market shifts, this way we can adapt quickly.

Organizational Risks:

- Departments may only focus on their specific goals, instead of cooperating with other departments towards an organizational objective.
- Over-relying on key employees for critical tasks may lead to issues in the future if these individuals were to either become ill or leave the company.
- Failing to identify potential risks during project planning may result in unexpected challenges and issues, which lowers the chances of the project being a success.
- By documenting progress we can reduce the dependency of individuals.

Financial Risks:

- The budget may fail due to underestimating costs, with hidden expenses and unexpected challenges not considered.
- Cash flow issues may arise if project payments are delayed, or if expenses are higher than predicted.
- Investments in technology may become invaluable due to swift advancements or changes within the industry.
- By being aware of certain risks like these, we can set aside a portion of the budget.

Risks and Mitigation

Risks	Mitigation
Technical Risks: Hardware failure, network issues	Redundant systems and regular maintenance, cloud-based backups, network monitoring.
Security Risks: Cyberattacks, social engineering	Multi-factor authentication, protocols, staff training. intrusion detection systems, regular pentesting.
Project Risks: Scope creep, integration issues	Agile project management, change management process, regular stakeholder reviews.
Organizational Risks: Lack of leadership continuity, high employee turnover	Strong internal communication, define clear roles, implement succession planning and leadership.
Financial Risks: Budget overruns, cash flow issues	Conduct regular financial audits, prioritize scalable solutions, build an emergency reserve, diversify funding.

Conclusion and recommendation

We recommend Option 3, the Hybrid Disaster Recovery solution. This solution leverages both on-premises infrastructure for enhanced data security and control, while utilizing cloud based services for scalability and rapid recovery capabilities. This approach provides flexibility and scalability for our business in case of future changes.

The hybrid approach also offers better cost-effectiveness compared to a fully cloud-based solution while maintaining robust security measures. Our cost-benefit analysis indicates that this solution will provide the best return on investment over the five-year period, with projected savings in both operational costs and downtime reduction.

Success criteria
How do we know that the goals are achieved? (External for the Project)

- Compliance with regulatory or security standards
    - Alignment with ISO 22301, GDPR and NITS cybersecurity frameworks.
- Business Continuity Readiness
    - Systems and infrastructure are able to remain operational during incidences and archives minimal downtime
- Security Resilience
    - Effective implementation of security measures which are tested
- Stability
    - Backups system and failovers are operating seamlessly

Benefits realization plan
A benefits realization plan helps the project deliver certain values to customers and employees. These values are improved system reliability, security and satisfaction for the customers.

- *Market*
    - Our hybrid approach ensures minimal disruptions to business, which allows products to hit the market without delays.
- *Satisfaction & trust*
    - Based on our project we are focusing on security and faster recovery time. This means that customers won't experience data loss, which builds trust.
- *Employee satisfaction & efficiency*
    - By having automated backup systems it means that the employees won't be depending on manually monitoring the infrastructure systems. This allows the employees to focus on innovation within other fields.

This plan helps the project deliver great value when it comes to business continuity, security and efficiency. By regularly tracking these points, companies can focus on long term benefits.

Funding and Status Overview
Funding and status refer to the financial planning, budgeting, and allocation of resources for the project. Below, we will explore the current status of funding and the financial strategies being considered.

Current Funding Status

- A *cost-benefit analysis* was conducted earlier, providing insight into expenditures and gross profit.
- *The Disaster Recovery and Business Continuity Project* is funded through:
    - Internal budget allocation
    - Potential service provider contributions
- *Financial projections:*
    - Initial investment: $33,500 USD
    - Recurring annual cost: $67,000 USD (over five years)
    - Expected profit: $131,500 USD (by reducing downtime, increasing efficiency, and enhancing cybersecurity resilience)

Funding Strategies

To meet the necessary financial requirements, a combination of internal and external funding resources will be utilized, including:

- *Bank Loans*
- *Credit Lines*
- *Venture Capital*
- *Private Investments*

Bank Loans

- A *structured loan* from a bank provides immediate capital but comes with obligations:
    - *Interest payments* can accumulate over time, increasing the financial burden.
    - *Failure to make payments* may compound the loan into a significantly larger debt.
    - *Collateral may be required* as security for the loan.

Credit Lines

- A *line of credit* provides access to funds as needed, offering greater flexibility in managing project expenses:
    - Unlike a lump-sum bank loan, a credit line allows borrowing *only when necessary*, reducing immediate debt obligations.
    - The bank sets an *approved limit* based on the organization's creditworthiness.
    - This approach is particularly suitable for the *Disaster Recovery Fund*, ensuring that financial resources are available on demand.

Venture Capital and Private Investments

- *Venture Capital (VC):*
    - Attracting VC funding can provide significant financial backing without the need for repayment.
    - Investors expect equity in return and may require strategic control over project decisions.
    - Suitable if the project has scalability and long-term revenue potential.
- *Private Investments:*
    - Angel investors or corporate partners may provide financial backing.
    - Typically involve equity sharing or revenue-based returns.
    - Ideal for organizations looking to expand disaster recovery solutions into a marketable service.

Financial Transparency and Accountability

- As the project progresses into advanced stages such as:
    - Implementing automated backup solutions
    - Establishing off site recovery centers
    - Integrating threat detection technologies
- An *updated cost-benefit analysis* will be conducted to ensure:
    - Funding partners remain informed on spending, timelines, and return on investment.
    - Financial strategies align with the evolving needs of the project.
    - Sufficient resources are available without compromising long-term sustainability.

Project Management Team

Project Manager:

- Responsible for the overall execution of the project, including managing timelines, coordinating the team, allocating resources, and ensuring effective communication across the team.
- The Project Manager ensures that the project stays on schedule, within budget, and achieves its goals.

Incident Response Manager:

- The main responsibility is to identify and respond to incidents, managing them as effectively as possible to ensure the organization can recover quickly from cyberattacks or IT crises.

- The incident response manager also has a key role in the development and implementation of the disaster recovery plan.

Business Continuity Manager:

- Develops and manages business continuity plans to keep essential operations running during and after a disaster.
- Works closely with IT and operations teams to ensure business recovery strategies align with disaster recovery plans.

Disaster recovery & Cybersecurity specialist:

- Develops security strategies, conducts risk assessments, and performs penetration testing to identify and address vulnerabilities
- Ensures that cybersecurity measures are built into disaster recovery plans to help prevent, detect, and respond to cyberattacks effectively.

System administrator:

- Manages and maintains the IT infrastructure, including servers, operations systems, and user management.
- Ensures system stability and availability by regularly monitoring and performing maintenance

Network engineer:

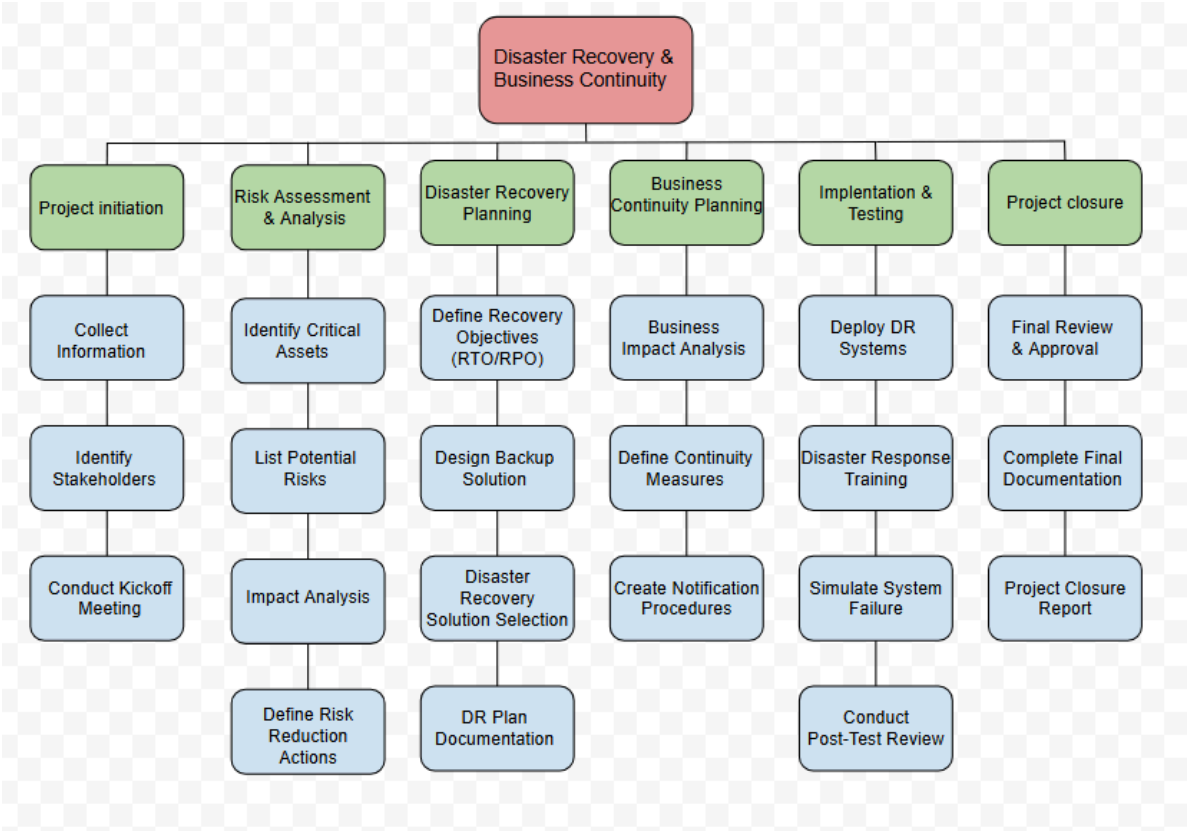
- Monitors and maintains the network infrastructure to ensure stable, secure communication, and high availability.
- Implements redundancy, firewalls, and security measures to reduce downtime and protect against cyberattacks.

DevOps engineer:

- Automates and optimizes infrastructure to improve efficiency and stability.
- Ensures quick recovery from failures using CI/CD and cloud solutions.

Assignment 6: Detail project plan

WBS:
The WBS breaks the project into manageable parts, with Level 1 as the project name, Level 2 as the main phases, and Level 3 as the tasks needed to complete each phase. This structure helps us plan, estimate time, and assign responsibilities more effectively.



Level 1: Project Name – Disaster Recovery and Business Continuity

Level 2: Main Phases

1. Project Initiation
2. Risk Assessment Analysis
3. Disaster Recovery Planning
4. Business Continuity Planning
5. Implementation and Testing
6. Project Closure

Level 3: Tasks

Project Resource Allocation Overview

The table below summarizes the key project roles, number of assigned resources, estimated effort in hours, and the main responsibilities for each role. This allocation ensures efficient project execution across planning, development, testing, deployment, and post-launch support phases.

Role	No. of Resources	Estimated Hours	Responsibilities
Project Manager	1	400	Overall project coordination, stakeholder communication, risk management.
Business Analyst	2	800	Requirements gathering, documentation, and analysis.
Software Developer	4	4,800	Code development, implementation of features, debugging.
UX/UI Designer	1	500	User experience and interface design, usability testing.
Tester/QA Engineer	2	1,600	Testing, bug tracking, quality assurance.
Security Specialist	1	400	Security assessments, vulnerability mitigation, compliance checks.

Deployment Engineer	1	300	Deployment of software, CI/CD pipeline maintenance.
Support Engineer	1	Ongoing	Post-launch troubleshooting, user support, maintenance updates.

Implementation & Testing: Effort and Cost Breakdown
We chose to focus on the Implementation & Testing phase because it plays a central role in the Disaster Recovery and Business Continuity project. This phase includes key activities like deploying systems, setting up backups, and testing recovery processes. It involves much of the technical work and cost, which makes it important for the project's success. It also ties in with other phases such as risk assessment and disaster recovery planning.

Effort Involved:
The implementation phase is complex and requires effort from multiple teams to ensure that the system is deployed efficiently. Since this is the first phase and is critical in the project.
It's vital that everything functions before deployment. This includes costs for maintaining the digital infrastructure. Such as:

- System Development: coding, configuring and integrating software
- Setup for Infrastructure: Maintenance of servers, databases and other security frameworks
- Security Validation: Running security checks such as penetration tests to identify vulnerabilities within the system.
- Deployment and monitoring: checking the system in a virtual environment and monitoring for issues.

Cost involved:
Cost breakdown is vital because each phase has a cost and a cost breakdown helps in allocating financial resources to where it's most needed. If this is not done it can lead to delays and unexpected expenses. By investing in the system it can achieve a higher stability, security and reducing risk in the later stages.

Cost Breakdown

- Development Costs: Salaries for developers, testers, and engineers.
- Software & Licensing: Cost of development tools, testing frameworks, and cybersecurity software.
- Hardware & Infrastructure: Expenses for servers, cloud storage, and networking components.
- Testing & Quality Assurance: Penetration testing, performance testing, and automated testing tools.
- Operational Costs: Maintenance, monitoring services, and ongoing security patches.

Category	Estimated Cost (USD)	Detail
Development Cost	$ 50,000 - $ 100,000	Salaries for developers, testers, and engineers.
Software & Licensing	$10,000 - $30,000	Development tools, cybersecurity software, testing frameworks.
Hardware & Infrastructure	$5,000 – $15,000 (per year)	Servers, cloud storage, networking components.
Testing & Quality Assurance	$15,000 - $40,000	Penetration testing, performance testing, automated tools.
Operational Costs	$5,000 - $15,000 (per year)	Maintenance, monitoring services, security patches.

Disaster Recovery Implementation: Effort and Cost Breakdown

Effort involved:
Disaster Recovery is essential for ensuring the continuity in the event of natural disasters, cyberattacks and system failures. A well designed Disaster Recovery plan minimizes downtime, which leads to a reduction in expenditure. Below are the stages involved:

- Risk Assessment & Planning – Identify threats, analyze business impact, and develop recovery strategies.
- Infrastructure & Backup – Deploy redundant servers, automate backups, and configure failover systems.

- Testing & Simulation – Run disaster recovery drills, test data restoration, and address vulnerabilities.
- Training & Documentation – Educate staff, create recovery guides, and assign response roles.
- Monitoring & Improvement – Implement real-time monitoring, update plans, and refine response strategies.

Category	Estimated Cost (USD)	Details
Risk Assessment & Planning	$10,000 - $25,000	Risk analysis, business impact assessment, policy creation.
Infrastructure & Backup Implementation	$30,000 - $60,000	Servers, cloud storage, failover systems.
Testing & Simulation	$10,000 - $25,000	Penetration testing, data recovery drills.
Training & Documentation	$5,000 - $15,000	Employee training, recovery manuals, role assignments.
Continuous Monitoring & Improvement	$5,000 - $20,000 (per year)	Security updates, system monitoring, performance reviews.

Testing and Simulation:
The estimations in this section are based on the Delphi technique, involving input from multiple experts to ensure accuracy. Additionally, these estimations are directly tied to resource allocation, considering both the number of personnel assigned to each task and their expected workload in hours. This ensures the budget and effort planning reflect realistic staffing needs for each work package.

Work Package/Task	Role	No. of Resources	Estimated Hours	Hourly rate	Cost (USD)
Penetration testing	Security Specialist	1	400-450	70	28,000 - 31,500
Vulnerability assessments	Tester/QA Engineer	2	600-650	55	33,000 - 35,750
Refine Protocols	System adminstrator	1	200	60	12,000
Validate RTO Compliance	Project manager	1	100	80	8,000

Review and Improvement:

Work Package/Task	Role	No. of Resources	Estimated Hours	Hourly rate	Cost (USD)
Stakeholder Review	Project Manager	1	200	80	16,000
Final System Deployment	Deployment engineer	1	300	60	18,000

Estimation Methodology

The Delphi Technique is used to estimate effort and cost, following Cadle and Yeates (2008, p.147).

Estimations:

- Each role, including project manager, security specialist, system administrators and Tester/QA engineer provided their estimates of effort for each work package/task. These estimates are provided anonymously.

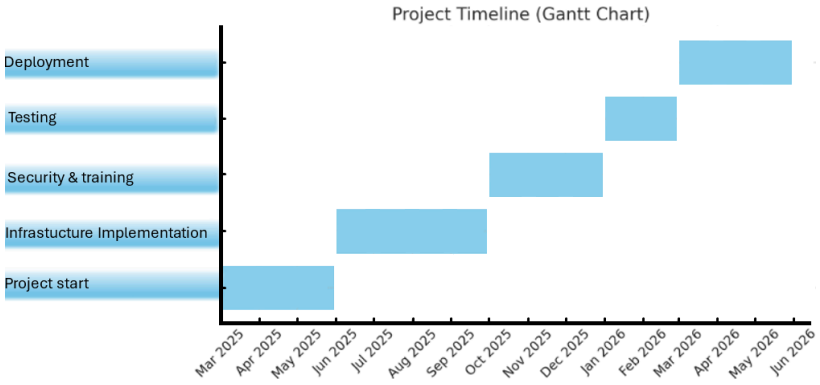
Review:

- The estimates are reviewed by each of the roles anonymously. These discussions should focus on the complexity of the hybrid on-premises and cloud-bases system, the changing nature of cyber threats and the spiral models emphasis in ongoing risk management.

Revised estimation:

- Each role is given the opportunity to reconsider their own estimates based on the summarised review from the previous stage.

Project timeline (12-15 months)



Phase 1: Project start

- Develop Project Initiation Document (PID)
- milestone: Project planning and getting approval
- Dependency: Must be completed before moving on to other phases

Phase 2: Infrastructure implementation

- Milestone: Set up Hybrid Infrastructure (on-premises & cloud)
- implementing security protocols (multi-factor authentication & encryption)

Phase 3: Security & training

- Train employees on disaster response.
- Conduct simulated attacks to keep employees sharp.
- Initiate real time monitoring and threat detection.
- Milestone: deployment of ai monitoring and staff training.
- Dependency: dependent on infrastructure implementation.

Phase 4: Testing

- Penetration testing to get an assessment of current state.
- Compliance with regulatory or security standards (ISO 22301 & GDPR).
- Ensure that all disaster recovery procedures are operational and functioning.
- Milestone: Testing & validating.
- dependency: Security enhancements must be complete.

Phase 5: Deployment

- Make a final project review and evaluation for the stakeholders to see.
- Deploy the operational plan & monitor.
- Milestone: Deployment and review.
- Dependency: Requires testing phase to be completed.

References

Victor, Kannada (2022, 22.june). Why you should use AES 256 encryption to secure your data. Progress. https://www.progress.com/blogs/use-aes-256-encryption-secure-data

International Organization for Standardization. (2019). *ISO 22401:2019 - Security and resilience - Business continuity management systems - Requirements.* ISO. https://www.iso.org/standard/75106.html

General Data Protection Regulation. (n.d.) *Complete guide to GDPR compliance.* GDPR. https://gdpr.eu/

Cadle, J. & Yeates, D. (2008). *Project management for information systems (5th ed).* Pearson Education Limited 2008

Assignment 7: Progress Report

Progress Report: Disaster Recovery and Business Continuity Project
Report Identifier: DRnBCP-Report-1
Date of report: August 2024

Period Covered:
This report covers the period from January 2024 to August 2024.

Summary of Progress:
The project “Disaster Recovery and Business Continuity Project” has reached the 50% milestone as of August 2024. We have completed Phase 1; project initiation, and have made notable progress into Phase 2; infrastructure implementation. Unfortunately, due to a major hardware failure in our backup infrastructure, we had to delay Phase 3; Security and Training.

With Phase 2 completed targeted for September, 2024, the plan is to fully initiate Phase 3.

Completed Milestones and Deliverables:

P1: Project Initiation

- Project Initiation Document (PID) successfully completed and approved.
- Comprehensive risk assessment finalized and documented.
- Project planning phase concluded with approval from all stakeholders.
    - Established a hybrid approach combining on-premises and cloud infrastructure for optimal disaster recovery.
- Risk and Security Analysis Completed.
    - Conducted a Risk and Security analysis and a SWOT analysis, identifying:
        - Strengths – Scalable infrastructure, improved security, reduced downtime.
        - Weaknesses – High initial setup costs, resource-intensive .

P2: Infrastructure Implementation

- Hybrid infrastructure (on-premises and cloud) fully deployed.
- Security measures, including multi-factor authentication and encryption, implemented and operational.
- access control, and real-time alerts to significantly enhance system security.

- Secure backup solutions did get configured but had a setback due to hardware failure.

P3: Security and Training

- Disaster response training sessions have begun for a few of the employees. Remaining training for the remaining employees is currently delayed.
- Real-time monitoring and threat detection systems installed and activated.
- Security monitoring and solutions deployed and validated by cybersecurity experts.

Effort and Costs to Date (Including Estimates)

Effort Involved:
At the 50% milestone, significant effort has been allocated across multiple roles, particularly in infrastructure deployment, security validation, and disaster recovery planning. The estimated and actual hours spent across different roles have been assessed, ensuring that the project is progressing as planned.

Role	**No. of Resources**	**Estimated Hours**	**Actual Hours Used**
Project Manager	1	400	380
Business Analyst	2	800	750
Software Developer	4	4,800	4,500
UX/UI Designer	1	500	480
Tester/QA Engineer	2	1,600	1,550
Security Specialist	1	400	420
Deployment Engineer	1	300	290
Support Engineer	1	Ongoing	Ongoing

- *Infrastructure Deployment:*
  Approximately 60% complete, with the remaining work focused on cloud integration refinements.
- *Security Validation:*
  75% of penetration tests have been conducted, with additional tests scheduled to address identified vulnerabilities.
- *Training & Awareness:*
  60% of employees have undergone cybersecurity training, with revised sessions planned for remaining staff.

Costs Incurred to Date and Estimated Outturn

Category	Estimated Cost (USD)	Actual Cost to Date (USD)	Projected Cost at Completion
Development Costs	$50,000 - $100,000	$48,000	$95,000
Software & Licensing	$10,000 - $30,000	$14,000	$28,000
Hardware & Infrastructure	$20,000 - $50,000	$35,000	$50,000
Testing & Quality Assurance	$15,000 - $40,000	$20,000	$38,000
Operational Costs (per year)	$5,000 - $15,000	$7,000	$15,000
100% Completed Project Cost	$100,000 - $235,000	124,00	$226,000

- *Infrastructure Setup:*
  Higher costs than projected due to additional hardware requirements and cloud licensing fees.
- *Security & Testing:*
  On track, but future penetration testing rounds may slightly increase costs.
- *Training & Operational Expenses:*
  Currently under budget, but additional sessions and monitoring may raise costs closer to the upper estimate.

Projected Cost at Completion

- Total Estimated Project Cost: $105,000 - $220,000
- Projected Cost Based on Current Trends: $210,000
- Variance: +5% due to unexpected security and infrastructure expenses.

Budget Adjustments & Mitigation Strategies

- Reallocation of Funds: Excess resources from non-critical areas have been redirected toward security and infrastructure costs.
- Cost Optimization: Vendor negotiations and phased implementation strategies have been implemented to prevent further budget overruns.
- Operational Efficiency Measures: Optimization of cloud-based services to reduce recurring infrastructure costs.

Problems encountered and potential control actions
Scenario: Technical issues

During the implementation of our disaster recovery and business continuity plan, we faced a critical server failure in our backup infrastructure. The failure was caused by a hardware malfunction in our main data center, making the backup systems temporarily unavailable. This resulted in delays in planned testing and revealed weaknesses in our redundancy, highlighting the need for improvements.

Impact on the project:

- *Delays in project timeline* - Since the backup system was down, key disaster recovery tests could not be conducted as scheduled, delaying the testing and validation of recovery protocols.
- *Increased costs* - Additional resources were needed to replace the hardware and fix the issue, impacting the project budget.
- *Risk exposure* - The downtime exposed critical systems due to inaccessible backups and weak redundancy, highlighting the need for a stronger failover system to ensure continuous availability.

Control actions taken:

- *Replaced faulty hardware* **-** Damaged server components were identified and replaced to restore backup functionality.

- *Improved Redundancy Strategy* - We analyzed the incident and updated the disaster recovery plan with additional failover mechanisms to prevent similar failures in the future.
- *Monitoring and alerts* - Added a monitoring system to quickly detect issues and send alerts for faster responses**.**

Way Forward **-** As we move into the final phases of the Disaster Recovery and Business Continuity Project, the primary focus will be on the full implementation of Phase 3: Security and Training, scheduled to commence in September 2024. This includes completing cybersecurity training for all employees, finalizing penetration testing, and validating the effectiveness of real-time threat detection systems. In parallel, we will conduct a comprehensive review and refinement of our failover and redundancy strategies, ensuring maximum system resilience. Regular progress evaluations will be carried out to keep the project on track and within budget. The goal is to reach 100% completion by December 2024, with a fully functional, secure, and sustainable disaster recovery solution in place.

References:

Cadle, J. & Yeates, D. (2008). *Project management for information systems (5th ed).* Pearson Education Limited 2008

Assignment 8: Risks and Mitigations

Risk register

By following our risk management strategy, we can easily find the risks that could impact our disaster recovery and business continuity project. By using Schimdts at al.'s checklist (2001) and Boehm's top-10 risk item tracking (1991) we can assess risks based on the possibility of them occurring and the impacts they might bring.

The table below is our representation of our risk register. The table includes:

- *Risk ID* - ID for each risk.
- *Risk description* - Brief explanation of the potential risk.
- *Category* - The type of risk (technical, security, financial, operational).
- *Likelihood* - Rated from low (1) to high (5).
- *Impact* - Rated from low (1) to high (5).
- *Strategy* - Risk response approach: Avoid, Transfer, Mitigate, or Accept.
- *Mitigation Strategy* – Actions taken to reduce or manage the risk.

ID	Description	Category	Likelihood	Impact	Strategy	Mitigation strategy
Risk 1	Hardware failure with backup	Technical	5	5	Mitigate	Implement redundant systems and real-time monitoring.
Risk 2	Cloud downtime	Technical	4	4	Transfer	Using more than one cloud provider.
Risk 3	Weak focus on disaster recovery plan	Organization & operational	3	4	Mitigate	Regular drills and improved protocols.
Risk 4	Attack on critical systems	Security	5	5	Mitigate	Usage of firewalls, AI and RTO.
Risk 5	Breach by phishing	Security	5	4	Mitigate	AI-based detection and employee training.
Risk 6	Budget cuts affecting security	Financial	3	4	Accept	Prioritize essential security upgrades.

Attack on Critical Systems:
An attack on critical systems such as Databases, Servers or the other parts of the network could seriously damage a business's operations, thus resulting in downtime which could cause downtime that translates into lost revenue in the millions. For example if this were to happen to a hospital, it could cause loss of life in a critical situation. Statistically speaking power outages dramatically raise mortality rates for hospitals, such as Hurricane Irma in Florida mortality rates rose by 25 percent in that event.

Impact On The Project:

- Disruption of Operations:
  Critical services could go offline, which would lead the company to stop key practices such as transaction processing and supply chain management.
- Monetary Loss:
  The longer there is downtime the more revenue is lost and in the event of an extended downtime may result in millions lost, such as Maersk did in 2017.
- Security Breach:
  Attackers could steal or corrupt data that is sensitive, resulting in losing consumer trust. This could involve ransomware, phishing, malware and so on.
- Difficulty of Recovery:
  Global systems are complicated and integrated which means they are harder to fix and recover slower. This is especially true for cloud and on premise systems.

Risk Recommendations for the project:

- Employ a Zero Trust Architecture:
  A security model needs to be implemented that ensures not one single person is trusted by default. This will limit lateral movement during a security breach.
- Redundant Systems :
  Having redundant systems in place ensures that a single point of failure won't happen. This would entail employing critical systems over a multitude of geo-locations across the globe.
- AI monitoring and Threat Detection:
  The state of the art in artificial intelligence used to train models for real-time threat detection and an implementation of a strategic threat response.
- Cyber drills:
  Having the network segmented so critical systems are isolated from potential breaches, this way the attacker will have a localized attack vector and not be able to access the entire system.

Conclusion:

By continuously monitoring these risks and following our mitigation strategies, we can guarantee minimal disruptions and an overall boost in strength when it comes to the infrastructure. Keeping this table updated will ensure that threats are addressed with security in mind.

References:

Cadle, J. & Yeates, D. (2008). *Project management for information systems (5th ed).* Pearson Education Limited 2008

Assignment 9: Stakeholder Analysis

This document outlines critical roles of the internal and external stakeholders as well as system administrators involved in the development and execution of our Disaster Recovery and Business Continuity Project. Each stakeholder group contributes a unique expertise to ensure the system's reliability, security and aligns with the goals of our organization. We made this stakeholder analysis because we needed to understand who would be affected: to help identify individuals and groups who could be affected by or have an influence over the success of this project. Also this would help us anticipate resistance or even support: A stakeholder analysis is key for managing expectations, understanding conflict and mitigating that.

- *IT & Project Manager*
- *System Administrators*
- *System Administrators*
- *Cybersecurity Team*
- *Employees*
- *Investors*
- *Investors*

Key internal and external stakeholders

Internal Stakeholders:
IT & Project Manager
Responsible for leading the technical development and managing the overall progress of the project. This includes ensuring that the system is technically solid, secure, and aligned with the company's requirements. They also oversee timelines, whether the project stays within budget, and coordination across the team to make sure the project stays on track and delivers expected results.

System Administrators
Responsible for managing and maintaining system operations, including backup systems, servers and network infrastructure. They also handle the configuration of the disaster recovery plan and are directly involved in its daily operations.

Cybersecurity Team
They are responsible for the security of the organization's systems and play an important part in integrating the disaster recovery system. They also help protect against threats such as phishing and cyberattacks.

Employees
Employees are end users who rely on access to systems and data to do their jobs. They expect minimal downtime and clear communication during issues.

Investors
Investors care about the company's finances and reputation. They expect the project to reduce risk and improve long-term stability.

External Stakeholders:
Cloud Provider:
Provides cloud services for storage, backup, and recovery. They are expected to deliver stable service and respond quickly during outages.

End-users (customers):
Customers expect reliable and secure services. During issues, they want fast recovery and clear communication to maintain trust.

Internal Stakeholders – Stakeholder Analysis Table

Stakeholder	Interest	Power	Expectations & Concerns	Engagement/communications
IT & Project Manager	High	High	**Expectations:** Completion of project milestones, adherence to budget, secure efficient use of resources & **Concerns:** Risks not addressed accordingly, delays that impact overall delivery.	Provide status reports about milestones,adherence to the budget and resource gain.

System administrators	High	Medium	**Expectations:** Having clear guidelines for system setup and maintenance, give manageable workloads, sufficient training and resources & **Concerns:** System downtime, changes to the system configurations, hardware failure	Technical briefings, clear documentation, support channels for internal communication
Cybersecurity team	Medium	High	**Expectations:** Robust Security protocols, timely identification and mitigation of risks, compliance with cybersecurity standards. & **Concerns:** Potential vulnerabilities, breaches in security infrastructure, insufficient testing	Regular security reviews, cybersecurity briefings, detailed vulnerability report and notification of security incidents.
Employees	Medium	Low	**Expectations:** User-friendly systems, No to minimal disruption to tasks, adequate training and support &	Updates via newsletters or other internal portals, feedback through surveys or forums. Scheduled training sessions and meetings.

			Concerns: System complexity, inadequate training, disruption of workflows, reliability and performance issues.	
Investors	Medium	High	**Expectations:** Project profitability, transparency on the project progress, achievement of the financial milestones. & **Concerns:** Financial risks, cost overruns, delayed return on investment, insufficient transparency in reporting.	Financial updates, investor meetings, detailed project performance reports and other regular updates.

External Stakeholders – Stakeholder Analysis Table

Stakeholder	Interest	Power	Expectations & Concerns	Engagement/communications
Cloud Provider	High	Medium	**Expectations:** Clear service requirements, secure and stable infrastructure, timely payments, effective issue communication & **Concerns:** SLA violations, unexpected downtimes, unclear requirements, miscommunication	Establishes a formal communication channel through weekly/bi-weekly meetings and shares. Also ensure that fast and transparent communication during any infrastructure incident or downtime is achieved. Provie post-incident reviews and continuous positive feedback loops for improvement.
End-users (customers)	High	Low	**Expectations:** Reliable, fast, and secure system; intuitive UI; responsive support & **Concerns:** System outages, poor usability, slow performance, data privacy issues	Provide updates through newsletters, platform notifications and other status updates. Offer support in the form of helpdesk access,chatbots and other app related support. Run security awareness about data privacy concerns for the customers.

Stakeholder analysis of power (influence) and interest:
Stakeholders play a critically important role when it comes to decisions, outcome and the overall success of a project. Understanding their power (influence) and interest is essential for effective management. Power refers to a stakeholders influence within project decisions and resources needed for a successful implementation. One with high power can make great changes, while those with low power have limited impact on the project.

Interest can be defined as a certain level of concern that the stakeholder might have with the project's success or failure. stakeholder with high interest are more affected by the outcome then those with low interest.

Stakeholder	Power (influence)	Interest	Comments
IT & Project Manager	High	High	The manager is responsible for planning and meeting the goals of the project. The manager also has influence over the project team. This gives the manager high influence since their role is tied to the success of the project
System administrators	Medium	High	They manage the IT infrastructure and help implement technical components.
Customers	Low	Medium	Customers rely on the outcome for their needs. The reception of the project is dependent on their feedback.
Employees	Low/medium	High	Limited with decision making, but highly affected by the project outcome
Cybersecurity team	High	Medium	The team helps ensure high security and protection against threats
Investors	High	Medium	Investors provide financial backup. Great influence, but not involved like other stakeholders.

Understanding stakeholders power and interest ensures great communication and mitigation of risk throughout the project. By categorizing the stakeholders as in the table we can align our strategies with their needs and desired outcomes.

Communication Channels and Strategies:
In the context of our disaster recovery, business continuity and infrastructure implementation project, it is a critical success factor that effective communication is held. Effective communication is essential to ensure that the proper communication channels are implemented. In project management this is a critical success factor. Given the rise of ever growing cyber threats, tech delays and stakeholder involvement. We recommend a structured communication approach that prioritizes things like swiftness, clarity and aligns with our stakeholders expectations. Disasters can escalate very rapidly so it is our goal that the right information reaches the right people at the correct time. Concise communication improves team coordination, improves clarity and allows us to recover quickly and strengthens our governance and control.

Our strategy is built around four pillars:

1. Rapid incident awareness and escalation.
2. Clear project visibility and milestone reporting.
3. Staff training and continuous learning.
4. Strong alignment between internal, executive, and external stakeholders.

Each communication channel is tailored specifically to each stakeholder group's levels of influence and interest. We incorporated the Essential Business Communication Channels, adapted to fit stakeholders needs and communication risk management:

1. In-person Communication (used for critical stakeholder meetings or post-incident reviews)
2. Phone calls (direct escalation of incidents)
3. Email communication (structured updates and documentation)
4. Video Conferencing (project planning, external partner coordination)
5. Text Messaging (urgent alerts, internal notifications)
6. Social Media (external communication during PR-sensitive crises)
7. Internal Newsletters (general employee updates, non-urgent news)
8. Team Chat (day-to-day collaboration using tools like Slack or Teams)
9. Webinars (staff training, awareness sessions, live Q&A)

Each of these pose a different set of challenges and risks. For example, a chat would seem a straightforward way to go about things but unless it is fortified, and access is

only granted to authorized personnel you may have a fiasco such as you are seeing on the news, in current day Washington. Also chats are not ideal for audits because they do not provide a formal, traceable communication trail that complies with regulatory standards, messages can be altered, edited and deleted. Which makes it difficult to reconstruct records for either a review or legal investigations.

Communications To Shareholders:
Shareholders are high-interest external stakeholders that have a high influence on the overall direction and stability of the company. Because of this, it is critical that our communication with them is clear, consistent and aligned with their expectations. Very much like suppliers and service providers expect reliability and standards compliance. Shareholders expect assurance that the project is being managed effectively and that the long term value is being protected. To meet these demands, our strategy includes the following focus areas:

1. *Regular Project Updates:*
   Shareholders will be kept informed of the project's progress, including updates on key milestones, delays, risk mitigation steps, and how these affect long-term value. This ensures transparency and builds trust.

2. *Compliance with Standards:*
   Shareholders will be updated on how the project aligns with internal and external guidelines such as ISO 22301 (business continuity), security protocols, and any other regulatory standards. This is similar to how app stores or service providers expect systems to meet guidelines and quality levels.

3. *Risk Management Transparency:*
   We will clearly communicate identified risks (like infrastructure issues or cyber threats) and what actions are being taken to control them. This mirrors how service providers expect fast and effective issue resolution.

4. *Reliability and Return on Investment:*
   Just like how suppliers are expected to deliver consistent resources, shareholders will be updated on how we're managing costs, securing infrastructure, and ensuring that the project stays on budget and delivers long-term value.

Conclusion
By integrating these communication channels thoughtfully, securely, and in alignment with stakeholder needs, we significantly reduce the risk of miscommunication, enhance response times, and foster a highly collaborative project environment.
This strategy directly supports our earlier goals of risk mitigation, staff preparedness, and stakeholder satisfaction. By integrating these communication channels thoughtfully, securely and in alignment with stakeholder needs, we significantly reduce the risk of miscommunication, enhance response times, and foster a highly collaborative project environment.

This strategy directly supports our earlier goals of risk mitigation, staff preparedness, and stakeholder satisfaction, while also ensuring that external expectations particularly those of shareholders, service providers, and regulatory bodies — are properly addressed.

By keeping shareholders informed through structured updates and clear alignment with standards like ISO 22301, we build long-term trust and demonstrate accountability. Overall, this communication strategy strengthens governance, improves project resilience, and contributes to the long-term success and sustainability of the initiative.
This strategy thereby contributes to the long-term success and resilience of the project’s success.

References:

Cadle, J. & Yeates, D. (2008). *Project management for information systems (5th ed).* Pearson Education Limited 2008

Assignment 10: Managing IT Project Change

Major Anticipated Change:
A major anticipated change in our project is the *strategic shift from a balanced hybrid infrastructure toward a more cloud-oriented architecture.* While the current model already combines on-premises and cloud components, the success criteria outlined in Assignment 5, particularly *improved downtime*, *business continuity readiness*, and *cybersecurity resilience*, suggest that cloud services will play an increasingly dominant role in future operations.

This shift will involve migrating *more critical infrastructure, data storage, backup systems, and disaster recovery processes to the cloud* to capitalize on benefits like:

- Reduced recovery time and improved RTO compliance
- Scalability for future growth
- Enhanced automation and AI-based monitoring
- Global redundancy and accessibility

However, this change also introduces *new technical, security, and operational challenges*, such as:

- Rewriting existing on-prem recovery protocols for cloud systems
- Staff retraining to adapt to new tools and workflows
- Greater dependency on third-party vendors
- Stricter compliance with cloud-related data privacy regulations

Ultimately, this change is essential to future-proof the business, and aligns directly with our goals of minimizing downtime, increasing resilience, and enabling long-term scalability as outlined in our success criteria.

The ADKAR Model and Timeline Management

The company is transitioning from on-premise systems to a more cloud-based system. This change affects how data is stored, how our systems are accessed, and how our employees work. This will involve new tools, protocols, and workflows, requiring targeted training and adoption.

To guide this change effectively, we are applying the *ADKAR* model, this is developed by Prosci - a proven framework for managing organizational change. *ADKAR* stands for:

- *Awareness*
- *Desire*
- *Knowledge*
- *Ability*
- *Reinforcement*

Each stage must be fulfilled to ensure successful adoption and implementation.

ADKAR Model Implementation Table

Stage	Timeframe	Objective	Impacted stakeholders	Key Points
Awareness	1-2 Months	Create awareness regarding the strategic shift.	All staff, especially general employees and executives.	Hold a project meeting and explain the shift to a cloud-based infrastructure. Show a brief presentation of the key benefits of moving to a cloud-based platform.
Desire	2-4 Months	Motivate and inspire the team to support the recent change.	General employees and IT-team	Motivate the team by connecting the change to fit the long-term goals of resilience, automation and scalability Implement a culture of change early on.
Knowledge	9-12 Months	Teach the IT-team how to adapt to the new cloud-based systems.	Security officers and IT-team.	Start training workshops, and provide access to the latest tools, backup systems and protocols. Inform the staff on how to access various cloud services such as AWS, Google cloud or Microsoft Azure

Ability	11-13 Months	Ensure staff has the ability to efficiently use the new systems, and evaluate performances.	General employees and IT-team.	Implement hands-on training for all team members. Assigning lead team members to coach other employees. Run disaster recovery drills.
Reinforce ment	13-15 Months	Praise the teams that most efficiently adapted to the new protocols .	Executive management.	Collect and provide feedback to resolve potential issues. Set up regular meetings for reinforcement and positive feedback. Monitor performance improvements. Incentivize teams who perform exceptionally.

Impacted stakeholders:
The strategic shift impacts a diverse group of stakeholders, including several key stakeholders whose involvement is critical to achieve project success.
If impacted, certain teams must learn and manage to use new monitoring tools and backup systems which would be a stark contrast from their daily workflows.
Employees for instance will experience temporary disruptions etc.
Down below you can see a list of teams and what their responsibilities are and how.

- *IT Teams & System Admins:* Responsible for maintaining both legacy and cloud systems. Their technical proficiency and buy-in are essential for a smooth migration.
- *Security Officers:* Key stakeholders tasked with ensuring data integrity, privacy, and compliance — their input is critical for setting up cloud-based controls.

- *General Employees:* May experience workflow disruptions, new protocols, and interface changes. Early awareness and motivation are essential to reduce resistance.
- *Executives/Management:* As budget allocators and project sponsors, their focus is ROI, long-term value, and project visibility.
- *Cloud Providers/Vendors:* Their SLAs, uptime guarantees, and security protocols directly impact our business continuity goals.

This stakeholder analysis aligns with and builds on the one presented in Assignment 7 and is reflected in our communication plan through targeted and frequent touchpoints for key actors.

Updated Risk Analysis in Light of Strategic Change:
These stakeholder concerns directly into several new and significant risks we've identified as a result of our anticipated shift to cloud infrastructure. Many of these risks build upon the earlier risk assessment outlined in Assignment 7 (pages 49 - 53), highlighting the importance of adapting our risk management strategy accordingly.

New Risk	**Related Previous Risk**	**Mitigation Strategy**
Downtime or data loss during migration	Migrating from older systems could lead to issues or data loss	Phased migration, full backups, rollback checkpoints
Increased exposure to external threats	Security concern: Cloud systems increase attack surface	Enforce encryption, zero-trust access, partner with secure cloud vendors
Staff resistance or skill gaps	Organizational risk: Over-Reliance on key employees	Modular training, assign cloud champions, create learning incentives
Unclear cloud vendor accountability	Compatibility/Integration issue	Clear SLAs, regular reviews, define backups vendors
Unanticipated cloud expenses	Financial risk: underestimated costs	Real-time cloud usage monitoring, auto-scaling. cost caps

These risks have been added to our updated risk registry, and mitigation strategies have been assigned to relevant project teams for tracking and resolution.

Communication Plan **-** To ensure all stakeholders are informed and ready throughout the transition from a hybrid infrastructure to a more cloud-focused disaster recovery architecture, this plan outlines a structured communication approach:

Stakeholder	**Information**	**Communication Method**	**Communication Timeline**
IT & Project Manager	Migration plan, goals, risks, and timeline	Weekly meetings, status reports	Before implementation
System Admins	Changes in backup systems and workflows	Workshop, email, documentation	During rollout
Cybersecurity Team	Security updates and threat handling protocols	Security briefings, meetings	Before implementation
Cloud provider	Roles, responsibilities and failover details	Email, SLA meeting	Before implementation
General Employees	Reduced downtime, improved usability	Email	1-2 weeks after launch
Investors	Business continuity improvements, ROI impact	Executive summary, reports	During rollout
End-users (customers)	Improved service availability and recovery speed.	Email	After launch

Conclusion

The transition toward a more cloud-based infrastructure is a critical change that aligns with our long-term goals of resilience, scalability, and operational efficiency. While it introduces significant risks and challenges, a structured change management approach (via the ADKAR model), an updated risk registry, and a proactive stakeholder communication plan ensure that we are well-positioned to manage this shift effectively. This change is not only strategic but essential to ensure the continuity and security of our IT operations in the years ahead.

References:

Cadle, J. & Yeates, D. (2008). *Project management for information systems (5th ed).* Pearson Education Limited 2008

Olmstead, L. (2024, December 18). *ADKAR Model: What Is It and How To Use It?* Whatfix. https://whatfix.com/blog/adkar-model-what-is-it-and-how-to-use-it/

Individual Reflection Note | kandidatnummer: 2

Contribution to the project

In this project I contributed by supporting the group's coordination and making sure we stayed organized and on track. I helped structure our workflow by suggesting how we could divide tasks fairly and set internal deadlines. I participated actively in group discussions and decision-making. My focus was on creating a good team dynamic where everyone was involved, and I tried to support others wherever it was needed.

Insights

Before this course, I had very little knowledge of project management. However, through this project, I've learned a lot of useful concepts and practices that I can hopefully take with me into future work environments. I've realized how important planning, structure, and especially communication is to deliver a successful result. Throughout this project, I've developed a much better understanding of how frameworks like PRINCE2 and agile help guide a project from start to finish.

Challenges

One of the biggest challenges our group faced was coordinating when and where to meet. With six members, each with different personal schedules and responsibilities, it was difficult to find a time that worked for everyone to meet physically. For the very first assignment, we managed to meet at school and work together in person. However, as the project progressed, it became harder to gather the whole group physically due to different commitments. To solve this, the group decided to start communicating using Discord. This made it much easier to stay in touch, divide tasks, and share updates, even when we couldn't meet in person. Although scheduling was a challenge, I think we handled it well by finding a flexible solution that allowed us to keep working together effectively.

Learning journey

Throughout this course and the project assignments, I've learned that successful project management depends on structure, adaptability, and good communication within the group. I also discovered how important it is to define clear roles and make sure that everyone knows what to do and is aligned with the project's goals.

One of my key takeaways for future project work is the importance of good teamwork and flexibility. Things will always change along the way, so the ability to communicate well and collaborate effectively is just as important as technical skills. This project has given me more confidence for future projects, especially when it comes to structure and collaboration.