PROJECT WORK: TECHY JAUNT CYBERSECURITY COHORT 4

CASE STUDY: BARNAAMAJ

GROUP: A

NAMES OF PARTICIPANTS

ABDULRAHMAN MUHAMMED

ABDULAZEEZ USMAN

TABLE OF CONTENT

EXECUTIVE SUMMARY

This project seeks to evaluate the strength and weakness of Barnaamaj a Tech Start Up, its potentials for growth, risk associated with carrying out its day to day business activities which could be detrimental to the said growth, its process and procedures, and ways to mitigate the risk associated with carrying out its duty as a Tech start up.

The project will focus on identifying both external and internal risks, such as cybersecurity threats, financial uncertainties, regulatory compliance challenges, and market competition, which could negatively impact the company's sustainability and growth trajectory. Additionally, the assessment will explore operational risks, including those associated with third-party vendors, scalability, and customer data management.

Conclusively, the project seeks to propose a strategic risk management plan to mitigate potential threats, ensuring that Barnaamaj is well equipped to handle operational challenges, safeguard its reputation and take advantage of new opportunities for growth. The risk management strategy will include improving security measures and vigilance, comply with industry standards and regulations, and implementing crisis management measures to ensure business continuity.

A

COMPANY OVERVIEW: BARNAAMAJ

Barnaamaj is an innovative tech startup that aim to revolutionize the primitive pilgrimage system for Nigeria Muslims wishing to travel to Saudi Arabia for Hajj and Umrah. The company function as a digital platform-designed to connect aspiring pilgrims with licensed and trusted Hajj and Umrah agencies, ensuring a smooth, transparent and secure Journey to the holy land of Mecca and Medina.

On Barnamaaj platform, potential pilgrims visit the website to search and find the best Hajj and Umrah deals for themselves and their loved ones. Upon getting finding a desired deal, they book a slot, make payment and get processed for their trips.

Key features of Barnaamaj includes, connection of Pilgirms with agencies and comprehensive support services from conception of ideas by pilgrims to travel to perform hajj till the pilgrims arrives.

Barnaamaj's mission is to create a more efficient and effective support platform for Hajj amd Umrah prospective reducing stress and uncertainties often associated with pilgrimage planning, allowing all pilgrims to fully focus on spiritual relevance of the journey.

Barnaamaj hopes to play a significant role in contouring the future of religious tourism in Nigeria, empowering muslims with cutting-edge technology with the aim of assisting muslims to fulfill one of the most important principle of their faith.

B

RISK ASSESSMENT FINDINGS: Barnaamaj

Due to the daily interactions of both internal and external users, the Barnamaaj website is vulnerable to various threats and has several weaknesses. Below are detailed risk assessment findings.

1) Security Risk

a) Threats:

Data Breaches: Barnaamaj website host sensitive financial and personal data (I.e names, passport details and payment information), there is a risk of data breaches due to hacking and unauthorized access.

Denial of Service (DoS) Attacks: attackers can flood Barnaamaj's server, making the platform inaccessible to users especially during Hajj and Umrah season when a lot of users are accessing the platform.

Ransomeware Attacks: Competitors can sponsor malicious actors to attack and lock Barnaamaj's data or system,demanding for payments before release.

Phishing and Social Engineering: Barnaamaj's platform could be exploited using this techniques to acquire personal information or inject malware.

b) Vunlenarabilities:

Lack of Two-Factor Authentication (2FA): makes it easy for attackers to gain unauthorized access to users accounts.

Weak Password Policies: on the part of partners and staffs could lead to unauthorized access.

Inadequate Data Encryption: Hackers can intercept and misuse account details of clients.

2) Compliance Risk

a) Threats

Non-Compliance with Data Protection Laws: As Barnaamaj operates both in Nigeria and potentially on an international scale, it is required to adhere to data protection laws such as the Nigerian Data Protection Regulation (NDPR) and the General Data Protection Regulation (GDPR) if serving clients outside Nigeria.

Violation of Religious Travel Regulations: Should Barnaamaj's partner agencies fail to meet the regulatory standards set by the Nigerian government or Saudi Arabian authorities for Hajj and Umrah services, the platform could face legal repercussions, penalties, or damage to its reputation.

Changes in Government Regulations: Unexpected changes in regulations, particularly those governing international travel or pilgrimage-related guidelines, could affect Barnaamaj's operations and necessitate swift adaptations to comply with new laws.

b) Vulnerabilities

Insufficient Regulatory Oversight of Partner Agencies: If Barnaamaj does not conduct thorough due diligence and continuous monitoring of its partner agencies, it risks collaborating with agencies that do not meet regulatory requirements, which could expose the platform to non-compliance penalties.

Inconsistent Record-Keeping: Failing to properly document customer agreements or transaction details could lead to non-compliance with tax, legal, or consumer protection laws, leaving the company vulnerable to legal issues.

3) Operational Risks

a) Threats

Dependence on Third-Party Agencies: Barnaamaj heavily relies on third-party agencies for essential services such as visa processing, travel arrangements, and accommodations. Any failure in the operations of these agencies—such as delays, subpar service, or unfulfilled commitments—could lead to a poor customer experience.

Service Interruptions: Technical problems, server downtime, or high traffic spikes could disrupt the platform's functionality, preventing users from booking or accessing services, resulting in lost revenue and customer dissatisfaction.

Poor Coordination with Agencies: If Barnaamaj fails to maintain effective communication with partner agencies, it may face issues like mismanagement of bookings, delivery of incorrect services, or delays in processing requests.

b) Vulnerabilities

Limited Control Over Partners: Barnaamaj's lack of direct control over its partner agencies exposes it to risks such as mismanagement, inefficiencies, or failures in service delivery that could affect its reputation.

Scalability Challenges: As Barnaamaj expands, its systems may struggle to handle increased traffic, particularly during peak periods like the Hajj season, potentially resulting in slow website performance, booking errors, or system downtime.

Staffing and Training Deficiencies: Inadequate staffing levels or insufficient training for customer service and technical support teams could hinder service quality, leading to operational inefficiencies and customer frustration

4) Financial Risks

a) Threats

Payment Fraud: Barnaamaj's handling of online transactions presents the risk of fraudulent activities, chargebacks, or credit card fraud.

Cash Flow Challenges: The timing mismatch between cash inflows from customer bookings and the payment deadlines for agencies or other business expenses could lead to liquidity problems.

Currency Exchange Fluctuations: Variations in currency exchange rates may impact the cost of foreign services, leading to unexpected price adjustments or financial losses.

b) Vulnerabilities

Weak Fraud Detection Mechanisms: If Barnaamaj's payment systems are not equipped with strong fraud detection tools, it may be vulnerable to unauthorized transactions and chargebacks.

Unreliable Payment Gateway: Issues with the payment gateway could disrupt transactions, causing delays, poor customer experiences, or financial setbacks.

5) Reputation and Brand Risks

a) Threats

Negative Customer Experiences: Unsatisfactory experiences, such as delays, poor service, or unresponsive support, may prompt customers to leave negative reviews or spread unfavorable word-of-mouth, damaging Barnaamaj's reputation.

Public Relations Issues: Problems in the pilgrimage process—like flight cancellations, visa issues, or poor accommodations—could lead to a PR crisis, undermining customer trust in Barnaamaj.

Cultural Sensitivity: Operating in the religious tourism sector means Barnaamaj must navigate cultural and religious sensitivities carefully. Any misstep in addressing these concerns could lead to backlash and alienate users.

b) Vulnerabilities

Insufficient Customer Service: If Barnaamaj lacks the resources to effectively handle customer complaints or inquiries, it risks leaving users dissatisfied, which could harm its reputation through negative reviews.

Overdependence on One Marketing Channel: Relying too heavily on a single communication or marketing channel (like social media) could damage Barnaamaj's brand if that channel faces issues (e.g., account suspension or negative feedback).

6) Technological Risks

a) Threats

Platform Downtime or Failure: Unexpected technical problems, such as server crashes or bugs, could render the platform inaccessible, particularly during busy booking periods, causing major disruptions.

Integration Failures: Barnaamaj integrates with various third-party systems (e.g., payment gateways, visa processing services). Any issues with these integrations could delay transactions, bookings, or service delivery.

b) Vulnerabilities

Outdated Technology: If Barnaamaj fails to keep pace with technological advancements, such as mobile optimization or enhanced security protocols, it risks becoming obsolete and losing its competitive edge.

7) External Risks

a) Threats

Natural Disasters: Events like earthquakes or floods in key pilgrimage locations such as Saudi Arabia could disrupt travel logistics and affect the pilgrimage experience.

Health Crises or Pandemics: Health emergencies, like the COVID-19 pandemic, could severely impact international travel, affecting both supply and demand for Hajj and Umrah services.

Geopolitical Instability: Political instability in countries like Nigeria, Saudi Arabia, or other transit nations could cause travel delays, cancellations, or safety risks for pilgrims.

b) Vulnerabilities

Reliance on External Partners for Logistics: Barnaamaj depends on airlines, hotels, and local service providers in Saudi Arabia. Any disruptions in these services—such as strikes, capacity limits, or logistical issues—could directly affect Barnaamaj's operations.

Conclusively, the risk assessment of Barnaamaj pinpoint several threats and vulnerabilities across functions, methods or mode, users, and operational activities. By proactively addressing these threats and vulnerabilities, Barnaamaj is guaranteed long term existence, success and operational sustainability.

C

Risk Management Plan: BARNAAMAJ

For the pupose of this project, the Qualitative Risk assessment method will be used to identify and access operational risk within Barnaamaj, evaluate effectiveness of controls put in place, and ensure risk management practices are adequate to mitigate identified risk. It fosters ownership at all operational levels and helps to improve Barnaamaj overall risk stance.

1.0 Risk Register- Barnaamaj

Company	Units	Risk Definition	Process	Control	Test Applied	Risk Rating
Barnaamaj	Customer Support	Risk Associated with provision of support and creation of customer experience for customers	Customer support and platform management	1. All customers inquiry and complaint are received from their social media hanles 2. Users request are made through the companys website. 3. Customers Documents are attached and verified as appropriate.	Reports are generated on monthly basis	Low
Barnaamaj	IT Security	Risk Associated with access management	Access Management	1. Customers register to gain access on Barnaamaj website. 2. A form is attached on Barnaamaj website for	Report of all users who onboarded on the website are generated on weekly	High

				proper onboarding.	basis	
Barnaamaj	Compliance	Risk Associated with Management of processes to ensure adherence to standards	Management of Regulatory Correspondence and standards	Mail communication as regards regulations are sent from time to time to units and department.	Monthly training is carried out.	Medium
Barnaamaj	Customer Support	Downtime on website & Network Unavailability	Customer support and platform management	Engage Technology team who manage the website.	Switch to manual process during downtime	Medium

1.1 Risk and Control Self Assessment (RCSA)

This is an important tool for identifying and assessing material operational risks and key controls in Barnaamaj. An effective RCSA helps to identify areas of exposure and optimize controls to minimize risk and achieve business objectives.

Period	Year	units	Control	Risk Definition	Test to be Applied	Test Result	Residual Risk Level	Action Plan
Q4	2024	Customer Support	1. All customers inquiry and complaint are received from their social media handles 2. Users request are made through the company's website. 3.Customers Documents are attached and verified as appropriate.	Risk Associated with provision of support and creation of customer experience for customers	Reports are collected manually by the officer in charge	Test Result show that the process in places is not sufficient enough	Low	Develop a robust platform that would be in sync with all support medium that will inturn give accurate report.
Q4	2024	IT Security	Customers register to gain access on Barnaamaj website. A form is attached on Barnaamaj website for proper onboarding	Risk Associated with access management	Report of all users who onboarded on the website are generated on weekly	Test Result showed that access management process is porous.	High	Infuse human detector and 2FA for all users onboarding on the website.

					basis			
Q4	2024	Compliance	Mail communication as regards regulations are sent from time to time to units and department.	Risk Associated with Management of processes to ensure adherence to standards	Monthly training is carried out.	Test Result shows that the current process is efficient but not effective enough	Medium	In addtion to mail communication, daily nuggest should also be shared with daily automated reminder.
Q4	2024	Customer Support	Engage Technology team who manage the website.	Downtime on website & Network Unavailability	Switch to manual process.	Current process is not efficient & effective.	Medium	Application should be developed to give room for alternative.

1.2 Key Risk Indicator (KRI)

This is a quantitative metric for monitoring Barnaamaj operational risk events to ensure that the risk events confirm with industry standard and Organizational risk appetite. It servers as early warning.

Frequency	Units	Risk Definition	Safety	Warning	Escalation Level	Risk Rating
Monthly	Customer Support	Risk Associated with provision of support and creation of customer experience for customers	1	2	3	Low
Monthly	IT Security	Risk Associated with access management	0	1	2	High
Monthly	Compliance	Risk Associated with Management of processes to ensure adherence to standards	1	1	2	Medium
Monthly	Customer Support	Risk Associated with Downtime on website & Network Unavailability	1	1	2	Medium

D

COMPLIANCE FRAMEWORK PLAN : BARNAAMAJ

Barnaamaj as a tech startup aim to simplify the Hajj and Umrah pilgrimage process for Nigerian Muslims. As a tech start up, its focus is connecting pilgrims with licensed Hajj and Umrah agencies. Barnaamaj must ensure its compliance with legal, regulatory, and industry standards. The primary objective of this compliance framework is to ensure that Barnaamaj operates within the legal boundaries, safeguarding the integrity of is website as it stand, its users, and its business partners.

1.0 Key Components of the Compliance Framework

Governance and Oversight	Policies and Procedures	Risk Assessment and Monitoring	Training and Awareness	Internal Audits
Barnaamaj should establish a Compliance Committee, led by a Chief Compliance Officer (CCO), responsible for overseeing compliance activities and ensuring that the platform adheres to relevant laws and regulations.	Barnaamaj should develop detailed policies covering data protection, transaction security, and customer handling, which will be communicated across all operational levels. Regular reviews will ensure that	Regular risk assessments, including RCSA (Risk and Control Self-Assessment) and the use of KRIs (Key Risk Indicators), will be utilized to monitor compliance with both internal policies and external regulatory requirements	All Barnaamaj employees, including third-party partners, will undergo ongoing compliance training to ensure they understand their legal obligations and the company's policies on data protection, financial	Regular internal audits will be conducted to assess the effectiveness of Barnaamaj's compliance controls. Findings from these audits will inform any necessary changes or improvements in the compliance framework

	these policies stay up-to-date with changing laws and business requirements		transactions, and customer privacy.	

1.1 Implementation Process

Assessment of Regulatory Requirements: Identify and document all relevant regulations that Barnaamaj must comply with (e.g., data protection laws, religious travel guidelines).

Creation of Compliance Policies: Develop internal policies for managing compliance, including data protection, financial reporting, and user safety.

Assigning Compliance Roles: Designate a Compliance Officer (CO) and ensure proper delegation of compliance tasks across departments.

Establish Monitoring and Reporting Systems: Implement automated compliance monitoring systems to track adherence to laws and internal policies in real-time.

Conduct Regular Audits: Audit compliance practices periodically and make necessary adjustments to ensure continuous alignment with laws and regulations.

Stakeholder Engagement: Engage regularly with external stakeholders (e.g., regulatory bodies, legal advisors) to ensure Barnaamaj remains compliant in a dynamic regulatory environment.

1.2 Risk Assessment Findings and Management

Barnaamaj faces several operational and security, as identified in the risk assessment. These risks are categorized and addressed as follows:

Security Risks

Threats: Data breaches, Denial of Service (DoS) attacks, ransomware, phishing, and social engineering.

Vulnerabilities: Lack of Two-Factor Authentication (2FA), weak password policies, and inadequate data encryption.

Mitigation: Strengthen security protocols with 2FA, improve data encryption, and implement robust fraud detection systems.

Compliance Risks

Threats: Non-compliance with data protection laws (e.g., NDPR, GDPR), violation of religious travel regulations, and changes in government regulations.

Vulnerabilities: Insufficient regulatory oversight of partner agencies, inconsistent record-keeping, and poor training programs.

Mitigation: Establish stringent due diligence processes for partners, maintain accurate records, and implement regular compliance training.

Operational Risks

Threats: Dependence on third-party agencies, service interruptions, and poor coordination with partners.

Vulnerabilities: Limited control over third-party agencies and scalability challenges.

Mitigation: Build stronger relationships with third-party agencies, invest in scalable infrastructure, and ensure regular communication.

Reputation and Brand Risks

Threats: Negative customer experiences, public relations issues, and cultural sensitivity challenges.

Vulnerabilities: Insufficient customer service and overdependence on a single marketing channel.

Mitigation: Enhance customer service and diversify marketing channels.

Technological Risks

Threats: Platform downtime, integration failures.

Vulnerabilities: Outdated technology.

Mitigation: Regular platform updates and invest in newer technologies.

External Risks

Threats: Natural disasters, health crises, and geopolitical instability.

Vulnerabilities: Over-reliance on external partners for logistics.

Mitigation: Develop contingency plans and diversify service providers.

E

CONCLUSION

It is safe to conclude that based on the assessment of Barnaamaj processes and operational flows various risk could hinder its continuous existence and performance as a tech start up. Regulations need to upwardly addressed, comlaince need to be reviewed and most importantly security needs to be straightened and loopholes blocked.

F

RECOMMENDATIONS

Based on assessment of Barnaamaj processes and activities, the following recommendations should be immediately implemented;

Customer Support Optimization: Barnaamaj customer support processed need to be fully optimized with platforms integrated with social platforms and website where the agents pick request and complaints from.

Enhanced Data and Platform Security: A human detected robot should be implemented on the website to identify if its human or robot that is accessing the website. Also, 2FA authentication should be implemented to protect all genuine users accessing the website.

Continuous Monitoring: Both RCSA and KRI should be regularly conducted to determine compliance and improvement levels based on how effective and efficient Barnaamaj processes are.

Training: Communications should be automated for regular reminders and educations on regulatory policies and update industry happenings.

Technological Advancements: A robust mobile Application should be built to serve as back up options for its website in cases of downtime and breakdown.

By implementing these recommendations, Barnaamaj can mitigate operational and compliance risks, leading to a more secure and efficient platform that continues to serve pilgrims with reliability and trust