Turbo

Nickodemus Konde, Shanyah Scott CYS 485

TURBO
CAR RENTAL

Table of Contents

● 1. Mission Statement (Shanyah Scott)

Turbo is committed to transforming the rental automobile industry by offering a smooth, adaptable, and practical platform that links renters and car owners. Our goal is to provide a wide range of vehicles to meet all needs, from daily commutes to unique excursions, all the while maintaining dependability, affordability, and top-notch customer support. We enable people to share their vehicles and facilitate travel while advancing the future of vehicle rentals.

● 2.1 Overview (Shanyah Scott)

Turbo is a platform that allows users to rent cars directly from automobile owners. Users can select from a large selection of automobiles offered by car owners, including standard cars, luxury cars, sports cars, and even electric vehicles, rather than going to a traditional rental firm. This business offers consumers a flexible and reasonably priced method to rent an automobile and is offered in many places throughout the United States and some other countries.

Turbo gives auto owners the opportunity to earn money by renting out their cars when they're not in use. The advantage of renting a car that suits their demands is that it's frequently less expensive than using a typical rental company. Turbo also offers insurance options to make sure both the automobile owner and renter are protected. Because it provides a more convenient and customized vehicle rental experience, the platform is growing in popularity.

2.2 Purpose of the Risk Management Plan (Shanyah Scott)

The risk management plan at Turbo is to identify, assess, and mitigate risks associated with its car sharing platform. It ensues safety and security of both hosts and renters by addressing potential liabilities, such as vehicle damage, accidents, and fraud. The plan helps maintain compliance with legal and regulatory requirements in various jurisdictions. While proactively managing risk, Turbo enhances customer trust which will help dominate in the competitive car rental market.

○ 2.3 Terms/Glossary (Shanyah Scott)

Cost-benefit analysis (CBA): A process used to determine how to manage a risk. If the benefits of a control outweigh the costs, the control can be implemented to reduce the risk. If the costs are greater than the benefits, the risk can be accepted.

Common Vulnerabilities and Exposures (CVE): Database of vulnerabilities maintained by the MITRE Corporation. MITRE works in conjunction with the U.S. Department of Homeland Security to maintain the CVE. The list includes over 40,000 items.

Denial of Service (DoS) attack: An attack designed to prevent a system from providing a service. A DoS attack is launched from a single client.

Disaster Recovery: The procedures to bring a system back into service after it has failed. Disaster recovery occurs after a disaster. Disaster recovery steps are documented in a disaster recovery plan that is a part of a business continuity plan.

Disaster Recovery Plan (DRP): A plan used to recover a system or systems after a disaster. A DRP is part of a business continuity plan.

Distributed Denial of Service (DDoS) attack: A DoS attack is an attack launched from multiple clients at the same time. A DDoS attack often includes zombies controlled in a botnet.

Intangible Value: Value that isn't directly related to the actual cost of a physical asset. Intangibles can include future lost revenue, client confidence, and customer influence. Compared to tangible value.

Risk Assessment: A process used to identify and evaluate risks based on an analysis of threats and vulnerabilities to assets. Risks are quantified based on their importance or impact severity. These risks are then prioritized.

Risk Management: The practice of identifying, assessing, controlling, and mitigating risks. Techniques to manage risk include avoiding, sharing or transferring, mitigating, and accepting the risk.

Profitability: The ability of a company to make a profit. It is calculated as revenues minus costs. Risk management considers both profitability and survivability.

Preventive Control: A class of controls identified by their function. A preventive control attempts to prevent the risk from occurring. For example, an unneeded protocol is removed from a server to harden it so that any attacks on this protocol are now prevented on the server.

Vulnerability: A weakness or exposure to a threat. The weakness can be in an asset or the environment. Controls mitigate risks related to vulnerabilities.

● 3.1 Assumptions (Nick Konde)

Reliable Platform Infrastructure: It is assumed that our infrastructure will be able to handle all customers within an appropriate time and provide excellent performance.

Third-Party Services Remain Available: Payment gateways, identity verification, and tracking services will operate reliably without major outages.

Employee Training is Effective: Turbo employees will be properly trained on security protocols and system usage to prevent and recover from any issues that may occur

Admins Use Secure Devices: Admins and remote employees access the system using company-approved devices with the proper security configurations.

Users Follow Security Policies: Employees, owners, and renters will not share passwords or fall for phishing attacks.

Financial Information Protection : Users assume that their personal information, including payment method, would be protected.

Vehicle Safety : Vehicle owners place their faith in Turbo that their vehicle will be returned safely

Extent of IT Security Measures : The users assume that when using this platform, they are not putting their personal information at risk of being assessed without their authorization or knowledge.

○ 3.2 Constraints (Nick Konde)

Firewall & Access Control: Only authorized users (renters, owners, employees, and admins) can access specific parts of the system, enforced via firewalls and role-based access controls

Firewalls & VPNs Function Properly: Firewalls, VPNs, and encryptions will operate correctly without major disruptions

Backup & Disaster Recovery: System backups must be performed regularly, but recovery time should be within an appropriate time frame

User Device Compatibility: The platform must support desktop, mobile, and tablets while having minimal errors and a consistent user experience across all platforms

Users Have Internet Access: Renters, owners, and employees have a stable and consistent internet connection to use the platform.

Database Defense : To avoid an SQL injection attack, the IT department will validate input and place emphasis on the use of prepared statements and conducting various penetration tests.

Cyber Attack Simulation : Simulating cyber-attacks using white-hat, grey-hat, and occasionally black-hat hacking techniques to test the security of our user data protection system.

Encryption : Payment information will be encrypted during data storage and retrieval.

Theft Protocol : A tracking system will be placed inside the vehicle that Turbo will be able to monitor if the rental period is exceeded. The tracking information will be made available to the local police department and the owner of the vehicle if the set agreement is violated.

Payment Verification Period : To avoid fraud and returned payments, there will be a verification period between the purchase of the rental vehicle and the date the vehicle will arrive to ensure the payment is complete and authorized.

○ 3.3 Risk Management Process (Shanyah Scott)

Finding possible hazards that could have an impact on the business is the first step in the risk management process. Next, the likelihood and impact of those risks are assessed. Strategies to reduce, transfer, accept, or avoid the risks are created after they have been evaluated. After that, the strategy is implemented, with regular reviews and modifications to guarantee efficient risk control during the undertaking. To keep hosts and renters aware and on the same page regarding risk management efforts, clear communication and comprehensive documentation are crucial.

To make sure the risk management plan is still applicable, the team should periodically examine and evaluate new and existing risks. Early risk identification and proactive response depend on departmental collaboration. The organization can better anticipate difficulties and minimize possible operational disruptions by cultivating a risk-aware culture.

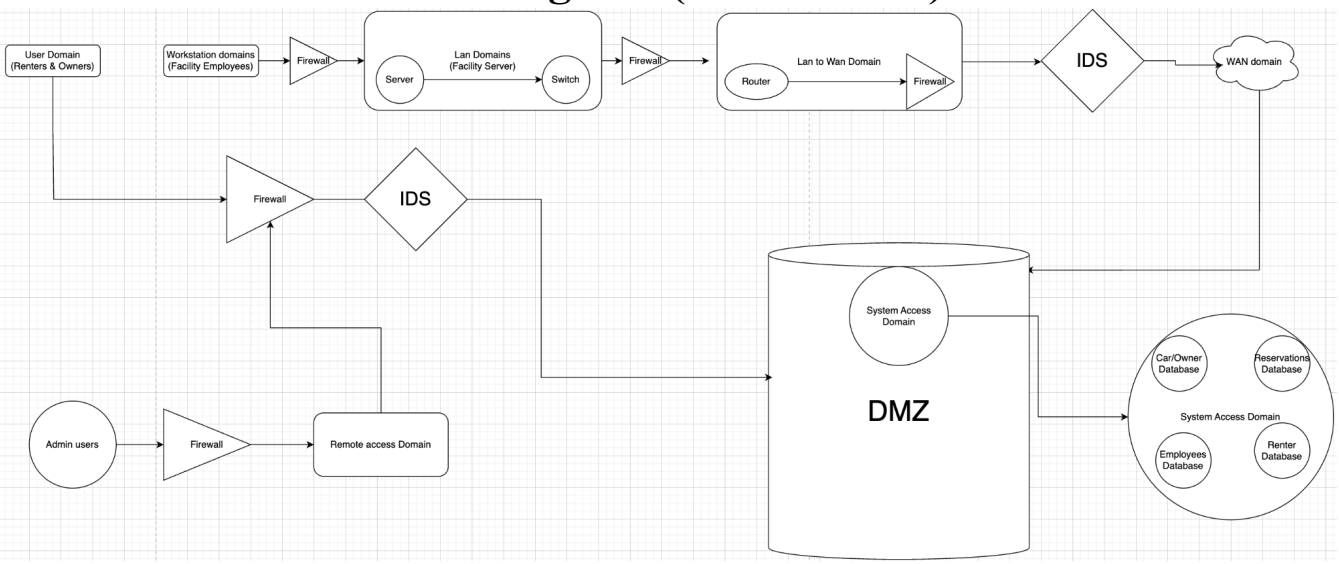
○ 3.4 Roles & Responsibilities (Shanyah Scott)

Name	Role	Responsibilities
Shanyah Scott	Risk Management Manager	Finding, evaluating, and reducing possible risks that can affect an organization's operations, financial stability, or reputation is the responsibility of a risk management manager.
Host	Owner of Vehicle	To give renters excellent experience, a Turbo Car Host oversees selling their vehicle, determining the price, and keeping the vehicle in good condition. In order to provide customer service, they handle reservations, plan pick-ups and drop-offs, and interact with visitors. They also must deal with routine maintenance, cleaning, and refueling in addition to

Name	Role	Responsibilities
		controlling possible hazards like insurance claims and vehicle security. To draw in more tenants, successful hosts maintain excellent ratings, optimize their listings, and reply to questions promptly.
Shanyah Scott	Project Manager	By establishing the product's vision, strategy, and roadmap, a product manager is in charge of directing the development of a product from conception to launch. To make sure the product satisfies client demands and corporate goals, they work with cross-functional teams that include engineering, design, marketing, and sales
Nick Konde	Fleet manager	Keep an eye on a company's automobile fleet and making sure it is well-maintained, economical, and efficient. They oversee fuel use and adherence to safety rules while coordinating the purchase, upkeep, and repairs of vehicles. To increase productivity and save operating expenses, fleet managers also monitor vehicle performance, plan routes, and put policies into place. They also collaborate with drivers to make sure that corporate rules are followed, and they could employ telemetry devices to keep an eye on fleet activity and boost output.
Mechanic	Vehicle Maintenance	A vehicle maintenance mechanic is in charge of examining, identifying, and fixing a range of mechanical and electrical problems in automobiles, trucks, and other vehicles. They maintain cars in top condition by doing regular maintenance like tire rotations, brake replacements, oil changes, and engine tune-ups. Mechanics diagnose issues and make sure all repairs adhere to performance and safety standards by using specialized tools and diagnostic equipment
Nick Konde	Network Analyst	Overseeing the operational and digital facets of a Turbo car-sharing company. They are responsible for keeping the fleet listed on the site, making sure pricing policies are reasonable, and improving search engine rankings. To stop fraud or abuse, they keep an eye on client interactions, booking activity, and security settings. They might also use remote access tools, GPS tracking, and

Name	Role	Responsibilities
		automated systems to improve security and expedite vehicle management while guaranteeing adherence to Turbo's policies
Jane Doe	Human Resource (HR)	would oversee the company's human resources operations and making sure Turbo's employees are properly supported and in line with its corporate objectives. Along with creating and putting into practice HR policies and processes, this also includes hiring, onboarding, and training new hires. In addition, they would oversee benefits administration, maintain adherence
Nick Konde	Marketing Manager	Creating and implementing marketing plans to advertise a business's goods and services and increase brand recognition is the responsibility of a marketing manager. To develop successful campaigns, they manage market research, examine consumer behavior, and pinpoint target audiences. To guarantee consistent messaging across several marketing channels, including digital, social media, and traditional advertising, they work in tandem with the sales, product, and design teams.
Shanyah Scott	Trust and Safety Analyst	Responsible for making sure hosts and visitors on the platform are safe and secure. To keep users safe, they keep an eye out for and investigate possible fraud, disputes, and policy infractions. Working closely with clients and internal teams to handle issues, this role entails data analysis, report evaluation, and tool used to spot suspect activity. By offering suggestions for system enhancements, they also guarantee that the platform conforms with legal and regulatory requirements and aid in enhancing safety procedures.

- **4.1 Infrastructure Diagram (Nick Konde)**



4.2 Detailed Explanation (Nick Konde & Shanyah Scott)

The network structure has many parts, and each part has different security layers. The User Domain is for renters and owners, while the Workstation Domain is for facility employees. Both connect to the internal LAN (Local Area Network) through firewalls to make sure access is controlled. Data and traffic in the local area network (LAN) are managed by a server via a hub. Firewalls and a router manage traffic between the LAN and the wide area network (WAN). The Application Server handles user requests to the System Access Domain, where several databases for cars, owners, reservations, employees, and renters are found. To ensure greater data security, each database is divided to block unauthorized access.

To manage remotely, Admin Users securely connect to the network via a VPN (Virtual Private Network) that is associated with the Remote Access Domain. There are numerous firewalls strategically positioned throughout the network that guard against unauthorized access and potential threats. This isolated configuration, coupled with VPN and firewall security, constitutes a robust security system that ensures sensitive data remains secure and is accessible only to authorized users.

- **5.1 Primary Threats (Nick Konde & Shanyah Scott)**

Component	Intentional	Unintentional
Credit Card Fraud	Stolen credit card information used for fake bookings.	User accidentally enters incorrect payment details.

DDoS Attack	Attackers overload our platform to disturb.	Firewall settings cause service slowdown.
Stolen/Fake Identity Accounts	accounts with fake identities to commit fraud or harm vehicles.	Mistyping of personal information during signup.
Personal Data Breach	Hackers steal customer data for identity theft.	Employee accidentally sends sensitive data in an email.
Vehicle Theft & Fraudulent Claims	A renter steals a vehicle and files a false claim.	Host forgets to lock the car, leading to theft.
Platform Vulnerability	Hackers exploit interfaces weaknesses to gain access.	Developer unknowingly introduces a software bug.
Unencrypted Data Transmission	Hacker intercepts sensitive data during transmission.	Employees use an unsecured WIFI connection for work.
Weak Authentication Mechanisms	Attackers exploit weak passwords to gain access.	Users do not enable two-factor authentication.
Vehicle Tracking & Privacy Risks	Hackers manipulate GPS tracking data.	an outage with the tracking system affecting data.
Insider Threats / Social Engineering	Employees intentionally misuse access privileges.	Employee falls for a phishing attack and shares login details.

(**Shanyah Scott)**

Credit Card Fraud: We would categorize credit card fraud as a medium to high threat, as we have implemented security measures such as fraud detection and verification systems to reduce risk. However, since our company facilitates person-to-person interactions, it remains an ongoing concern.

DDoS - Distributed Denial of Service: Distributed Denial of Service (DDoS) is considered a medium threat because a flood of traffic from multiple sources can severely disrupt the platform's servers, potentially damaging the service and harming its reputation. To mitigate this risk, we can implement advanced DDoS protection measures.

Stolen/Fake Identity Accounts: We would classify this as a high threat, as the use of fraudulent information can lead to illegal activity. While we have verification measures in place to reduce the risk, it remains a challenge that could still occur, especially concerning personal data.

Vehicle Theft and Fraudulent Claims: This would be considered a high threat because stolen vehicles and false damage claims not only pose a risk to the company but also negatively impact the host, potentially driving them to seek services from competitors that offer better protection in such situations. Even with verification and insurance measures in place, the high value of the vehicles makes it a significant threat to the company. This includes risks related to stolen vehicles, damage or theft fraud, and fake insurance claims.

Platform Vulnerability: Platform vulnerability is a high threat because a breach or malicious attack could expose user data, payment information, or lead to system manipulation, resulting in significant losses for everyone involved. While security measures are in place, the risk remains for any online platform, especially with potential flaws on the website and malware attacks.

Unencrypted Data Transmission: Unencrypted data is a high threat to us because if sensitive payment information and personal data are not properly encrypted, malicious attackers could gain access, leading to data breaches, identity theft, and financial fraud. To mitigate this risk, encryption protocols will be implemented to secure the data, especially since we handle payment and sensitive information. If personal information isn't encrypted through the proper third-party channels, it becomes vulnerable to man-in-the-middle attacks.

Weak Authentication Mechanisms: This is a high threat because without proper authentication, the risk of unauthorized access to user accounts and misuse of the platform increases. This remains a significant security concern. Implementing 2-step authentication will help address this issue and strengthen security. Additionally, it adds an extra layer of protection, ensuring that only authorized users can access sensitive information. By requiring a second form of verification, we reduce the likelihood of unauthorized account access.

Vehicle Tracking and Location Privacy Risk: Vehicle tracking and location privacy is a medium to high threat because, while tracking helps ensure the safety of rented cars and prevent theft, it can also raise privacy concerns. Balancing security and privacy will be a top priority to minimize this threat. The use of geolocation data could lead to potential privacy breaches if not carefully managed, so it's essential to implement strong safeguards to protect user information.

Insider threats or Social Engineering: This is a medium to high threat because employees could potentially misuse their access, and through social engineering, both employees and users may be tricked with fake promotions or manipulated into releasing their personal data, usernames, and passwords. Employees may inadvertently give out sensitive information, manipulate data, or make mistakes in their code. Additionally, employees could become targets of attacks aiming to gain access to internal systems, which could cause significant harm to the platform or its users.

Legal and Liability: This is a high threat due to the legal issues related to accidents and damages. Violations of local laws can result in lawsuits that could harm the company’s reputation and financial standing. Legal risks are significant, especially with the unlawful use of vehicles, young drivers, and inadequate insurance coverage, all of which increase the likelihood of costly legal challenges.

Basic Phishing Scams: This is considered a medium threat because we have strong security measures, such as email filters and fraud detection systems, in place to identify and block phishing attempts. Additionally, regular training and awareness programs for employees help them recognize and avoid phishing tactics, minimizing the chance of falling victim to such scams. While it's always a concern, our preventive strategies significantly reduce the likelihood of a successful phishing attack.

Minor Software Bugs: Minor software bugs are considered a low threat for Turbo Business because they typically do not cause significant disruptions to operations or compromise sensitive data. These bugs are often quickly identified and resolved by our technical team, ensuring minimal impact on our platform's performance. Additionally, our regular software updates and testing processes help prevent small issues from escalating into larger problems, maintaining the overall stability of the system.

○ 5.2 Impact Table (Shanyah Scott)

Threat	Impact Level
DDoS	Medium
Stolen/Fake Identity Accounts	High
Vehicle theft and Fraudulent Claims	High
Platform Vulnerability	High
Unencrypted Data Transmission	High
Weak Authentication Mechanisms	High
Vehicle Tracking and location Privacy Risk	Medium to High
Legal and Liability	High
Insider Threats/Social Engineering	Medium
Credit Card Fraud	High
Basic Phishing Scams	Medium
Minor Software Bugs	Low

○ 5.3 Compliance Organization (Nick Konde & Shanyah Scott)

Transportation & Vehicle Regulations (Nick Konde)

- Department of Motor Vehicles (DMV) Compliance: Ensures all vehicles are legally registered, meet state safety standards, and have valid plates.
    - Require owners to upload valid registration documents before listing a vehicle.

    - Conduct quarterly audits on vehicle registrations and send reminders before expiration.
- **National Highway Traffic Safety Administration (NHTSA) Compliance:** Overseas vehicle safety standards, crash test ratings, and recalls ensuring vehicles meet national safety laws.
    - Require owners to check recall status and upload proof of repairs before listing. Implement an automated recall alert system to flag vehicles with unresolved issues.
- California Air Resources Board (CARB) Compliance: Enforces California's strict emissions laws, ensuring vehicles meet environmental regulations before being rented out.
    - Require smog test results for all vehicles listed in California. Prevent non-compliant vehicles from being rented in restricted areas.

Insurance and Consumer Protection (Shanyah Scott)

- **State Departments of Insurance Compliance:** Regulates insurance coverage, ensuring Turbo provides legally required protection for owners and renters.
    - Logging incident reports before and during rental
    - Provide liability insurance to the owner
    - Turbo assures compliance with State Departments of Insurance requirements by offering the legally needed coverage for owners and renters in all states where it operates. Keeping up with new laws, collaborating with insurance specialists, and maintaining adequate documentation all assist to assure continued compliance. Also, teaching employees on insurance standards reduces errors and ensures that activities comply with legal requirements. (Shanyah Scott)
- **Federal Trade Commission (FTC) Compliance**: Protects consumers from deceptive business practices, ensuring Turbo provides transparent pricing and fair policies.
    - Display the calculations that go into the price before a purchase is made
    - Inform the user of the fees that are included: additional cleaning, new driver, late return, etc.
    - Informing users of all factors that result in a denial of service: Failure to pass a background check, drug test, failure to pay a deposit or fraudulent payment method, etc.
    - clear pricing and fair business practices. This entails accurately explaining fees, policies, and agreements to users while avoiding misleading claims. Regular assessments of marketing, pricing, and customer interactions assist to avoid misleading practices and maintain consumer confidence. (Shanyah Scott)
- **Consumer Financial Protection Bureau (CFPB) Compliance:** Regulates financial transactions, ensuring Turbo handles security deposits and payments fairly.
    - Monitoring transactional activities to try and find anomalies
    - Conduct a thorough investigation into all reports of incidents regarding unknown or incorrect charges.

- Provide constant updates throughout the investigation and what factors lead to the decision and steps to move forward to assure the customer's concerns are being prioritized.
- Ensure that security deposits and payments are handled fairly and openly. This involves offering explicit conditions, preserving user cash, and adhering to regulatory requirements for financial transactions. Regular audits and secure payment mechanisms assist to ensure compliance and consumer trust.(Shanyah Scott)

Data, Privacy and Cybersecurity (Nick Konde)

- California Consumer Privacy Act (CCPA) Compliance: Protects customer data, requiring Turbo to disclose, secure, and delete user information upon request.
  - Offer the consumer the option to have their data collected and respond to the customer's decision to access, delete, and opt-out at any time.
  - Provide training to staff on how to assure the customer has that discretion.
  - Assure that the privacy policy is clear and easy to understand so users understand what they are agreeing to along with.
  - Age verification

Employment & Business Operations (Nick Konde)

- Occupational Safety and Health Administration (OSHA): Ensures workplace safety for employees at Turbo's vehicle storage facility.(Nick Konde)
  - Conduct monthly safety audits and employee training. Provide proper protective equipment and emergency response plans
- Equal Employment Opportunity Commission (EEOC) Compliance: Prevents workplace discrimination, ensuring fair hiring and treatment of Turbo employees.
  - Set in place for employees with special needs
  - Remove race and gender from applications to reduce the chances of discrimination during the onboarding process
  - Conduct training that outlines the employee's protection against retaliation as well as the process of filing a complaint
- Internal Revenue Service (IRS) & State Tax Agencies Compliance: Requires Turbo to properly classify workers, file taxes, and report earnings.
  - Conduct a business audit to confirm that all taxes are filed and paid in full and reduce the chances of tax fraud being committed.
  - Track any outstanding liabilities or tax payment history that would fall under noncompliance.

○ 6. Business Impact Analysis (Nick Konde)

Critical Business Function	Impact of Disruption	Recovery Priority	RTO	RPO	Risk Score
Vehicle Booking, Return, and Check-In/Check-Out	Loss of revenue, customer dissatisfaction, operational paralysis	High	2 hours	1 hour	10/10
Secure Payment Processing	Immediate loss of income, inability to confirm bookings, potential customer loss	High	30 minutes	15 minutes	9/10
GPS Tracking for Monitoring and Safety	Impact on customer safety, vehicle recovery, operational efficiency	Medium	1 hour	30 minutes	7/10
Customer Support and Dispute Resolution	Increased customer complaints, loss of customer trust, reputational damage	Medium	4 hours	2 hours	6/10
Maintenance Scheduling for Vehicles	Vehicles may be unavailable due to missed maintenance, reducing fleet reliability	Low	12 hours	6 hours	5/10
Identification Verification for User Security	Unauthorized access to vehicles, security breach, fraud	High	1 hour	30 minutes	8/10

● 7. BCP (Shanyah Scott)

○ 7.1 Scope of the BCP:

This Business Continuity Plan (BCP) involves the critical parts of Turbo's operations that must remain in operation during a disruption. Functions for example booking a vehicle, payment (and payment information) security, vehicle tracking through GPS, customer support, vehicle

maintenance, and user verification. Relying on these services being operational allows for the protection of customers, the prevention of revenue loss, and risk mitigation. Like the original, the BCP is meant for all employees, contractors and the systems that support the functions of software, data storage, and communication systems. Coverage of these functions limits the duration of which business cannot operate, protects essential business functions, and organizes recovery when business activities have been disrupted.

○ 7.2 Business Continuity Strategy:

Turbo's business continuity plan outlines key actions for continuing business and restoring service should a service disruption occur. To remain resilient for its clients, Turbo has introduced redundancy in its systems by using cloud-based systems for both vehicle booking and digital payment processing that are also capable of having failover systems in case of a failure. Backup manual procedures have also been developed so clients can receive support using alternate methods of booking and payment if digital systems are unavailable. Employee readiness is another important aspect of the strategy. Employees have established training for emergency procedures including utilizing the backup communication system and the backup manual workflows. Furthermore, Turbo will keep communication and transparency with its users and clients. During disruption communication will be prompt and alternative options or compensation will be offered to reduce inconvenience and maintain service.

○ 7.3 Communication Plan:

Turbo's communication plan guarantees that both customers and employees are kept updated during a service disruption. With a communication plan in place, employees and customers are much more likely to understand the situation, and thus their confusion is reduced, and trust is kept alive. The internal communication plan is that Turbo will use a phone alert, or email alert to commence informing staff of the disruption. The IT team will send regular updates to management to keep everyone updated on the situation and actions taken to restore service. With external communication, customers will be informed through email, SMS messaging, and Turbo's social media feeds. It is important to be clear with customers on the issue and consequently how soon services will resume.

○ 7.4 Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO):

Critical Function	RTO (Recovery Time Objective)	RPO (Recovery Point Objective)
Vehicle Booking, Return, and Check-In/Check-Out	2 hours	1 hour
Secure Payment Processing	30 minutes	15 minutes
GPS Tracking for Monitoring and Safety	1 hour	30 minutes
Customer Support and Dispute Resolution	4 hours	2 hours
Maintenance Scheduling for Vehicles	12 hours	6 hours
User Identification Verification	1 hour	30 minutes

○ 7.5 Key Recovery Personnel and Roles:

Turbo's Business Continuity Plan depends on the dedication of individual team members as each person has different roles to fill in the event of a disruption. The BCP Manager is tasked with leading the entire recovery process of the incident and ensuring recovery steps are completed as planned to restore business operations efficiently. The IT Manager oversees bringing All Technology Systems back online such as, the website, databases and payment processing

systems. The Operations Manager priorities are focused on the continuity of core business functions, including vehicle bookings, Customer support services, and vehicle maintenance, with no interruption. Further, the Customer Support Lead is responsible for restoring the systems that support customer service as well as ensuring that the customer-base is continuously informed and provided with support during the incident. All these identified titles contribute to unique aspects to the recovery and necessary for an efficient and effective recovery.

○ 7.6 Plan Testing and Review:

Turbo will test the Business Continuity Plan (BCP) annually through a simulated disaster to ensure that the BCP will function as it is designed to. The simulated disaster allows Turbo to observe how well the teams react to the situation, whether our backups work as designed, and if there are any problems or weaknesses that will need to be addressed prior to the event happening in reality. Testing isn't the only important part of the business continuity plan, it will also be reviewed and updated annually, or sooner if Turbo makes any significant changes to its systems, services or non-profit structure. We will ensure that the BCP is frequently reviewed so that it is current and applicable to the company in the event of a disruption.

● 8. DRP (Nick Konde)

○ 8.1 Scope of the DRP:

The Disaster Recovery Plan (DRP) does one thing: Protect and plan to restore Turbo’s most critical IT systems (web servers, payment processing, GPS tracking, and all associated customer and business data as well as backup systems) in the event of a severe disruption. The DRP describes the steps that need to be taken to restore systems back online as quickly and as safely as possible and will identify the procedures needed to use backup systems substitution (i.e. failover) to maintain essential workflows while significant systems are being restored. The DRP will also outline how to effectively communicate with staff and customers to keep them updated through the recovery process. This ensures that in the event of technology failure, Turbo could recover within acceptable downtime limited impacts on its operations, data, and reputation.

○ 8.2 Key Components of the Disaster Recovery Plan:

Turbo's Disaster Recovery Plan (DRP) includes several core components to be sure key systems can be restored and the duration of downtimes reduced during an outage. The first component is the backup strategy Turbo employs to ensure every customer's data, vehicle status, and booking transactions are being executed to a secure cloud storage system. The backups are properly reviewed each month to ensure completeness and usable data. In the event of data loss, the data recovery process allows Turbo to restore critical systems (i.e. booking, payments, GPS tracking) from the most recent backup, and include built in procedures to minimize time loss. The second element is that Turbo's most important services (i.e. payment processing, booking, customer support) include redundant systems, so that in the event of system failures, the redundant systems in the cloud environment can immediately take over and minimize service interruptions with very little effort on Turbo's part and without too much effort from customers. Lastly, Turbo has set up failover systems where in the event Turbo's servers stop responding to requests, those requests automatically send to backup servers/platforms without need for human interruption. These elements ensure Turbo can and will continue to operate while serving customers and minimizing the effect of the problem, even in the face of a significant technical failure.

8.2.1 Alternate Site Strategy: Hot, Warm, and Cold Sites

Attribute	Hot Site	Warm Site	Cold Site
Location	Los Angeles, California	Austin, Texas	Raleigh, North Carolina
Purpose	Immediate failover	Mid-level disruption recovery	Long-term outage recovery
Capabilities	Fully operational with real-time data replication	Pre-configured hardware with regularly updated backups	Basic infrastructure; hardware and data brought in as needed
Recovery Time	Minutes (near-zero downtime)	1–2 hours	24–72 hours

Reason for Selection	Tech hub with robust infrastructure, connectivity and an hour away by flight	Centrally located, cost-effective, low disaster risk	Affordable region with reliable utilities and emerging tech scene

---

○ 8.3 Recovery Process:

Turbo Recovery Process gives the process for bringing the operations back up and running safely where it has been disrupted. The recovery process commences with disaster identification. The IT team immediately kicks off with a review of the disaster, what is the situation. They need to find out what caused the disruption, if it was system, software, or database corruption from a server crash, a SaaS data breach or a failure to provide services through the payment system. The second step if it was a disaster, is initial recovery actions. If the outcome of the review was a disaster/disruption, then the IT team must decide the fastest course of action they can take. The information they collect will be communicated upwards or to the stakeholders of the original incident. In the case of Turbo, the loss of a significant amount of data, the IT team would undertake immediate actions, which could include restarting servers, normalizing the outage against the existing disaster policy, returning to functioning backup cloud systems, or retrieving from secure backups.

Step three is restoration of services. The IT team should focus on the most important systems first to minimize financial losses, like payment processing and the overall booking system as the top priority as this is critical to any company, and Turbo would not want to lose money. Next, the GPS tracking and customer support operations should be restored so that Turbo knows their customers know where all the vehicles are, followed closely by a functional customer service-related support systems portal.

The last step is verification of systems; for all restored service systems, the IT team should take time to test to ensure functionality was reinstated correctly and/or was doing its job. The IT team checked everything worked safely including confirming payments transactions were happening, bookings could be made and that customer service tools are functioning properly.

○ 8.4 IT Infrastructure Recovery Priorities:

Critical Function	Recovery Priority	Recovery Procedure
Vehicle Booking, Return, and Check-In	High	Restore servers and database from backup.
Secure Payment Processing	High	Ensure the payment gateway is restored and the database is intact.
GPS Tracking	Medium	Restore GPS tracking systems and verify vehicle locations.
Customer Support	Medium	Ensure call, chat, and email systems are functional.
Maintenance Scheduling	Low	Restore vehicle maintenance scheduling system.

○ 8.5 Disaster Recovery Team:

The Disaster Recovery team at Turbo consists of key team members, with everyone playing a vital role in the return to operation of IT systems after a service disruption. The DRP Manager is responsible for step by step implementing the recovery process, indicating who completes each part of the plan and maintaining the lines of communication open and flowing within the team. The IT Support Lead role is focused on reconstructing a damaged technological state, supporting the restoration of key IT systems back to operational status and switching activity back to the backup cloud services provider should it be necessary to civil the service disruption. The Customer Service Support Lead is to bring all our customer service tools back online as soon as possible and update communications to customers as we recover. The Backup and Database

Administrator will be responsible for the restoration of all essential data back online from backup source storage. The team regarding storage must keep track of key items and data such as customer bookings, payment information and customer record for each customer, be sure the key activities are brought back and information integrity tested. In essence this small group of key team members will ensure that Turbo can return to activities as fast as possible and limit operational downtime.

○ 8.6 Communication During Disaster Recovery:

Effective communication plays a pivotal role in the disaster recovery process at Turbo. In terms of internal communication, all employees of Turbo will be communicated with either through email or the company communication tool. These communications will aim to inform employees of what has occurred, what systems are impacted, and the steps being taken for recovery. Further, the company will ensure that updates will be given in regular increments, which serves to help employees stay coordinated, reduce confusion, and generally remain aware of their roles in the recovery and restoration process. With regards to external communication, Turbo will communicate with customers through email, social media posts, and its company's website. These communications will explain the disruption that has occurred, the services that may or may not be unavailable, and when Turbo expects that those services are restored, if at all. Moreover, being noticed and timely is instrumental in preserving trust in the customer relationship and demonstrates that Turbo is acting to restore customer service.

○ 8.7 Plan Testing and Review:

To ensure the Turbo Disaster Recovery Plan (DRP) remains relevant and useful, the process includes ongoing testing and reviews. Each year the organization will perform disaster recovery exercises to stage an outage of systems, to allow the Team to rehearse their roles, record how long it takes to recover from a disaster, and identify gaps in the plan before a real disaster strikes. In addition to conducting the testing, the DRP will be reviewed and updated as required at least annually, or sooner if major changes have been implemented in Turbo’s technology, systems, or infrastructure, to keep the plan current, accurate, and available in support of the business in the event of business disruptions.