Part A

I. Integrity Controls

A. Input Controls

There are several controls that can be used in the Make Reservation through Web Interface use case. Because this use case utilizes a form that requires input, input controls will be vital to have in place. There are four main types of input controls that will be useful for this use case:

1. *Value limit controls*: Each input field on the reservation form should have a maximum limit of allowed values that is reasonable for the type of requested data. For example, there should be a maximum number of characters allowed for name fields, credit card info fields, etc. It is important to note that these value limits may vary based on geographical location and language used. If we assume the car sharing IS is Canadian and using the English language the following limits would be reasonable to impose:

firstName: 50 characters limit
lastName: 50 characters limit
emailAddress: 256 characters limit
phoneNumber: 8 character limit
creditCard: 12 character limit

Limiting input values to reasonable lengths prevents actors, either accidentally or intentionally, overloading a system with data or injecting harmful code.

2. *Completeness controls:* Addresses, names, and credit card information entered into the web reservation form must be complete to prevent data corruption in the system or errors with financial records or location records.

3. *Data validation controls:* Similar to completeness controls, some input fields should require a certain format to be validated. For example, phone numbers will need to be an approved format to be validated. Additionally, it is important that credit card information meets the standard format to ensure all the information is complete and that the credit card can be charged legally.

4. *Field combination controls*: These controls are important for times and dates in particular. The system should not validate any reservation that has retroactive dates or dates that go beyond the one-year limit for reservations that is outlined

in the documentation. Errors like this can cause data corruption and errors in the reservation system, as well as confusion for staff and customers.

B. Output Controls

Output controls ensure that any output from the web reservation process arrives securely at its intended destination. There are several different types of output controls that would be beneficial for this use case:

1. *Physical access to output*: Any printers that are utilized by the car sharing organization's staff should be adequately protected by physical controls such as locked offices, staff authentication to enter offices, security measures such as cameras, man traps, etc.

2. *Disposal of output documents:* The organization should have a clear policy and procedure on how to dispose of sensitive output information that aligns with the area's standardizations. For example, in the North America, NIST and ISTG-33 are organizations that publish standards for data retention and destruction. Typically for printed documents, this means shredding them.

3. *Access controls*: Access controls are a category of integrity controls on their own, but they also apply to output specifically. Only authorized and authenticated users should be able to access account information that is displayed on the web application. This applies to both customers and employees. Only authenticated users should be able to view reservation information.

4. *Labeling*: All output that is printed physically or displayed digitally should have appropriate labels attached. For printed documents, there should be an organization letterhead and labels to indicate the sensitivity of the information contained in the document. Digital files and data packages generated by the web reservation process should have internal labels including the source of the file, the content, users of the file and a time stamp. This helps to ensure non-repudiation.

C. Redundancy, Back-up and Recovery

Redundancy and back-ups help ensure the integrity of data in the case of hardware failure, disasters or malicious deletion or withholding of the data. Back-ups ensure that vital data is not lost in case of emergency and redundancy ensures that users have access to their data even if there is some failure with the system's hardware. Recovery is important in the case that back-ups and redundancy fail to protect the data.

Back-ups should be completed at times of low utilization because they use a lot of system resources. Additionally, backups should be done at times of low utilization to prevent data corruption. This would most likely be late at night, although that time frame may vary depending on use, as the car sharing IS is a 24/7 pilot project.

Redundancy is particularly important for a car sharing service because if the system fails, customers may be locked out of the vehicles they have reserved if the SmartCard or PIN systems are down. This would cause complications, potential safety concerns and a loss of confidence in the organization.

The car sharing IS can ensure that there is a redundancy plan in place:

1. Data stored in multiple locations, copies of the data stored in multiple different locations.

2. Spare essential hardware components and professionals available who can resolve hardware issues.

3. Data centers chosen in areas that are not prone to natural disasters.

4. Ensuring that all software has a rollback plan in case of failure.

D. Fraud Prevention

Fraud needs three things to occur: opportunity, motivation and rationalization. The latter two are difficult to control from a systems design point of view. The car sharing organization could ensure that employees are treated well to reduce motivation. The company could also include background checks in their hiring process to ensure that employees have no criminal records.

Opportunity is something that we can attempt to control with system design decisions. Opportunity to commit fraud can be reduced with the following methods:

1. Implementing a policy of least privilege. Every user of the system including employees and customers should only be able to access the least amount of data that they need to perform their functions. When a customer leaves the platform, they should lose all access to the system. Likewise, when an employee leaves the organization, they should also lose all access to the system.

2. The system administrators should have an Access Control List that is updated regularly.

3. Separation of duties should be enforced among the employees of the organization. No single employee should have ultimate access and control over sensitive data.

4. Documentation, records and audit trails should be meticulously kept.

5. Logs should be monitored, and a security team should be hired or sourced out to ensure that events and incidents are tracked and investigated.

6. Frequent penetration testing and other security tests should be employed to ensure that the system remains secure.

7. Access to physical offices and servers should be protected with physical controls such as locks, biometric entry, etc. Servers should be at a different location than the main offices.

8. Finally, education and training for all employees is vital to ensuring the security of the system and fraud prevention.

II. Access Security

A. Users

The car sharing IS is a pilot project, and recruitment is based on an invitation model, therefore controlling user access is simpler than if the project was fully open to the public. Safety measures still need to be taken, including monitoring the users of the system and maintaining an up-to-date Access Control List.

The users that are intended for the car sharing IS include employees of the organization and the customers. Customers consist of invited members and new members who were referred by current members. The following criteria must be met:

1. Among these users, only users whose applications have been approved by a manager should have access to the system.

2. During the application process, a manager should ensure that all approved users have valid licenses and have verified their identities. Additionally, insurance information should be validated.

3. The manager should ensure that invited members have local addresses to take part in the pilot project.

4. Any accounts that are inactive should be regularly purged and removed from the system.

5. Any accounts that have reached the maximum number of penalties should be terminated without delay.

6. User SmartCards should be monitored, and no ignition access should be given to a SmartCard holder without their personal PIN. Customers should be aware of the process for lost or stolen SmartCards, as well as educated on the importance of PIN confidentiality. The process of replacing a card or changing a PIN should be easily accessible to the customer.

Employees of the car sharing IS should meet the following criteria:

1. Authorized employees only, accessing the system based on least privilege and separation of duties.

2. Terminated employees should promptly lose access to the system.

3. Employees should not share access details with one another.

The car sharing IS is not designed for members who are not local to Futureville, terminated customers or employees, non-driver customers, or anyone under the age of 18.

B. Access Control List

ACL Legend:
R – Read
C – Create
E – Edit
D – Delete
X – Execute

Resource	Members	Clerical Staff	Assistant Manager	Operating Manager	System Admin	HR
Reservations	R C E D	R C E D	R C E D	R		
Member Accounts	R E D	R	R C E D	R		
Inventory	R	R	R E D	R C E D		
Billing	R	R	R C E D	R C E D		
SmartCard/PIN	X	R E D	R C E D	R		
Penalties	R	R	R C E D	R		
Fleet				R C E D		
Marketing				R C E D		
IT System				R	R C E D X	
Hiring				R C E D		R C E D

III. Storyboard

Storyboard for Make Reservation through Web Interface use case: