Risk Assessment Report

DART (Delaware Authority For Regional Transit)

Team 5

Mohammed Touheed Patel

Sameed Mirza

Eric Jhessim

Franciscar Irungu

Andrew Makau

Contents **Page Number**

1. Introduction

The Delaware Transit Corporation, operating as DART First State, is the only public transportation system that operates throughout the U.S. state of Delaware. DART First State provides local and inter-county bus service throughout the state and also funds commuter rail service along SEPTA Regional Rail's Wilmington/Newark Line serving the northern part of the state. The agency also operates a statewide paratransit service for people with disabilities. DART First State is a subsidiary of the Delaware Department of Transportation (DelDOT).

Although most of its bus routes run in and around Wilmington and Newark in New Castle County, DART operates bus route networks in the Dover area of Kent County; seven year-round bus routes serving Georgetown and Sussex County; and additional seasonal routes connecting Rehoboth Beach, other beach towns in Sussex County, and Ocean City, Maryland. In 2023, the system had a ridership of 8,034,800, or about 32,900 per weekday as of the second quarter of 2024.

DART was awarded the prestigious Public Transportation System Outstanding Achievement Award by the American Public Transportation Association in 2003.

2. Executive Summary

We are a team from the University of Delaware, MISY 650 “Security & Control” graduate students. We performed a comprehensive IT risk assessment for the company “DART”. The Delaware Authority for Regional Transit (DART) plays a pivotal role in providing public transit services across Delaware. The organization relies on a combination of physical, technological, and human assets to ensure efficient and reliable operations. This risk assessment evaluates 15 plus critical assets, identifies vulnerabilities, and proposes actionable mitigation strategies to enhance DART's operational resilience.

2.1 Purpose

The Delaware Authority for Regional Transit (DART) serves as a vital component of Delaware's transportation infrastructure, providing bus, rail, and other transit services to thousands of residents and commuters daily. With increasing reliance on technology and a growing threat landscape, the need for a comprehensive risk assessment has never been more critical. The primary goal of this report is to identify and evaluate risks associated with DART's operations, focusing on the physical, technological, and personnel assets. This report serves as a blueprint for improving DART's security posture, minimizing potential disruptions, and enhancing its ability to respond to and recover from adverse events.

2.2 Scope

i. Physical Assets: Buses, depots, transit stops, and rail infrastructure.

ii. Digital Assets: Ticketing systems, network infrastructure, and public-facing mobile applications.

iii. Human Resources: Drivers, operators, security personnel, and administrative staff.

iv. Processes: Scheduling, communication, and customer service operations.

3. Risk Assessment Approach

The risk assessment was carried out by a team of five consultants.

Name	Title
Mohammed Touheed Patel	Technology Risk Assessment Consultant
Sameed Baig Mirza	Technology Risk Assessment Consultant

Eric Jhessim	Technology Risk Assessment Consultant
Franciscar Irungu	Technology Risk Assessment Consultant
Andrew Makau	Technology Risk Assessment Consultant

By following the NIST SP 800-30 methodology: Asset Identification ,Threat and Vulnerability Analysis ,Risk Scoring and Prioritization ,Recommendation Development.

3.1 Initial Assessment:

The information-gathering process was conducted via a review of the documentation available on the website of DART that provided clear descriptions of the existing systems, user interactions, system integrity, network diagrams, and operational manuals related to systems. While looking at the documentation, we had the questions recommended by the National Institute of Standards and Technology(NIST) as a reference in mind to help us extract the right information. Supporting diagrams and system architectures were part of the documentation and have been used in conducting the risk assessment.

3.2 Data Collection and Documentation:

The data collection and documentation were tailored for business specifics, capturing insights related to current procedures, controls, user access processes, system integrity, database administration, and audit. Supporting documentation and flowcharts were foundational for the risk assessment.

3.3 Risk-level Metrics and Classification: A Risk-Level Metrics system was employed to generate risk ratings, categorizing them as Low (1 to 10), Medium (>10 to 50), and High (>50 to 100)

- **Low Risk:** Scores from 1 to 10. The company can decide whether to develop an action plan or accept the risk.

- **Medium Risk:** Scores between 10 and 50. While the system can continue operating, an action plan is required within a reasonable timeframe. Medium-risk issues are closely monitored as they can escalate.
- **High Risk:** A score higher than 50, necessitating immediate action. While the system can continue operating, an action plan must be developed and executed promptly.

This risk assessment approach equips Company DART to make informed decisions and implement necessary actions to fortify its platform against potential threats.

3.4 Risk classification:

Score	Rating
1 to 10	Low
10 to 50	Medium
50 to 100	High

3.5 Metrics table:

Risk Score = Impact x Likelihood

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	Medium 100 x 0.5 = 50
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 =100

4.System Characterization:

The Delaware Authority for Regional Transit (DART) operates a complex ecosystem of physical, digital, and human assets designed to deliver reliable public transit services. This section outlines the key components and functions of DART's operational systems.

Key Components

4.1 Physical Infrastructure:

- **Bus Fleet:** Over 300 buses equipped with GPS and communication systems.
- **Rail Lines:** Light rail system with 50+ miles of tracks, ensuring urban connectivity.
- **Transit Stops and Depots:** Over 5,000 transit stops and multiple depots for vehicle maintenance and storage.

4.2 IT Systems:

- **Ticketing Systems:** Digital payment and passenger management platforms.
- **Network Infrastructure:** Firewalls, routers, and servers for data exchange and operational control.
- **Mobile Applications:** Passenger-facing apps for ticketing, real-time tracking, and scheduling.

4.3 Personnel:

- Drivers, operators, administrative staff, and IT personnel ensure seamless operations.

4.4 Core Functions:

- **Scheduling and Dispatch:** Real-time communication for bus and rail scheduling.

- **Maintenance Management:** Systems for tracking and scheduling vehicle maintenance.
- **Customer Support:** Centralized systems for managing passenger inquiries and complaints.

4.5 System Workflow

DART integrates its physical and IT assets using advanced technologies like GPS, machine learning, and cloud computing. This enables efficient route planning, predictive maintenance, and enhanced passenger experience.

5. Threat Statement:

DART faces a wide range of threats, from cyberattacks to natural disasters. This section outlines the key threats, their sources, and potential impacts on operations.

5.1 Threats Identified

1. Cyber Threats: Phishing, ransomware, and hacking target DART's ticketing systems and network infrastructure.
2. Physical Security Risks: Vandalism, unauthorized access, and theft threaten DART's depots, vehicles, and transit stops.
3. Personnel-Related Risks: Insider threats, negligence, and lack of training in security practices.
4. Operational Risks: System failures, such as GPS outages and software malfunctions, disrupt services.
5. Environmental Risks: Hurricanes, floods, and extreme temperatures affecting physical infrastructure.

Threat Sources

- External Actors: Hackers, vandals, and competitors.

- Internal Actors: Negligent or disgruntled employees.
- Natural Causes: Weather-related events and natural disasters.

Potential Impacts

- Service disruptions, financial losses, and reputational damage.

6.Risk Assessment Results:

Using the Risk Assessment approach, we individually examined all the assets, threats, and vulnerabilities in addition to evaluating the likelihood and impact of each asset of DART. We then calculated the risk score of each asset.

High-Risk Assets:

Asset	Threat	Likelihood	Impact	Risk Score
Ticketing Systems	Cyberattack	High	High	90
Mobile Applications	Data Breach	High	High	70
Autonomous Vehicles	GPS Spoofing	High	High	70

Medium-Risk Assets:

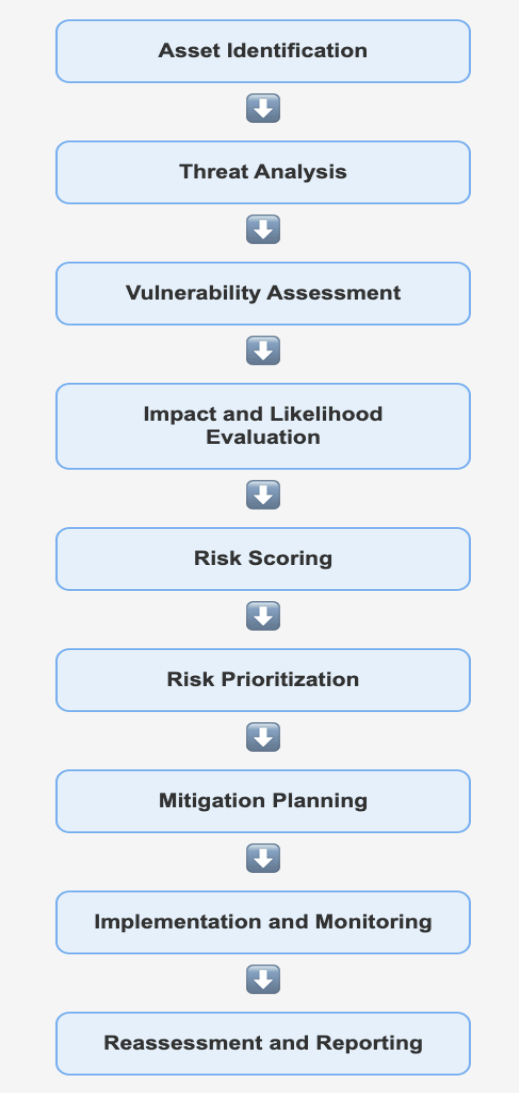
Asset	Threat	Likelihood	Impact	Risk Score
GPS Systems	GPS Spoofing	Medium	Medium	30
Communication Networks	Signal Jamming	Medium	Medium	25
Security Cameras	Network Intrusion	Medium	Medium	25

Low-Risk Assets

- Collaboration tools and reporting systems were classified as low risk due to limited potential for widespread or high impact (we found no low risk assets).

You may look at Appendix B for full details on the risk statement for each asset in DART

7 . Appendix A : Process Flow Chart



8. Appendix B : Risk table

Asset	Threat	Vulnerabilities	Likelihood	Impact	Risk Score
Central Control Hub	Cyberattack	Weak access controls, Outdated software	0.9	High	90
IoT Sensors	IoT Exploitation	Insufficient encryption, exposed ports	0.8	High	80
Autonomous Vehicles	GPS Spoofing	Lack of anti-spoofing technology, outdated GPS	0.7	High	70
Mobile Applications	Data Breach	Weak user authentication,Insecure data storage	0.7	High	70
Communication Networks	Signal Jamming	Unencrypted data transmission, unprotected communication channels	0.5	Medium	25
Cloud Storage	Cloud Misconfiguration	Insecure Cloud Storage settings, Improper data access control	0.6	High	60
Ticketing Systems	Ransomware	Lack of malware detection, outdated software	0.8	High	80
Data Centers	Physical Breach	Insufficient physical security, lack of surveillance	0.7	High	70

Security Cameras	Network Intrusion	Weak network configuration,outdated security protocols	0.5	Medium	25
GPS Systems	GPS Spoofing	Lack of encryption, reliance on GPS only	0.6	Medium	30
Vehicle AI Systems	AI Exploitation	Unsecured AI models, inadequate security testing	0.8	High	80
Backups Systems	Data Corruption	Incomplete backup process, no real-time monitoring	0.6	High	60
Threat Detection Systems	Malware	Insufficient monitoring, outdated antivirus software	0.7	High	70
Collaboration Tools	Third-party Risks	Insufficient vetting of third party integrations	0.5	Medium	25
Emergency Systems	Inadequate Response	Poor incident response planning, outdated protocols	0.6	High	60

9. Appendix C : Basic System Architecture

DART's IT and operational architecture integrate multiple systems and processes, as detailed below.

Frontend Components:

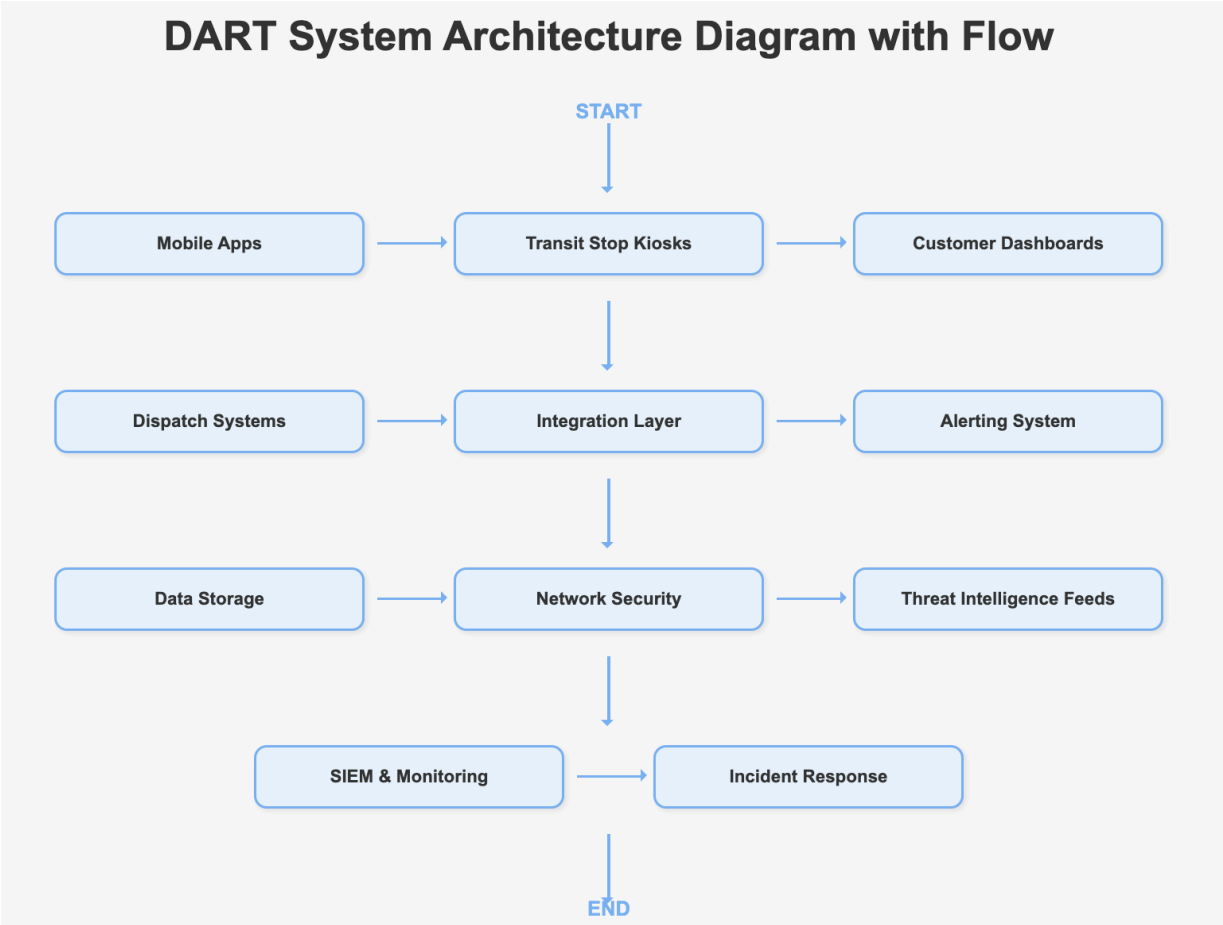
- Passenger Interfaces: Mobile apps and kiosk systems for ticketing and scheduling.
- Administrative Dashboards: Tools for operational management and monitoring.

Middleware:

- Dispatch Systems: Connect buses, depots, and rail services for real-time updates.
- Integration Layers: API connections between ticketing systems, GPS, and network services.

Backend Systems:

- Network Security: Firewalls, intrusion detection systems (IDS), and endpoint security.
- Data Storage: Secure databases for passenger, scheduling, and financial data.



10. Recommendations

To keep DART's assets safe and secure, it's important to take a practical and focused approach. For ticketing systems, this means keeping the software up-to-date and encrypting payment and passenger data to prevent breaches. Adding multi-factor

authentication (MFA) and performing regular security checks will help keep everything running smoothly and securely.

For the network infrastructure, having properly set-up firewalls and intrusion detection systems (IDS) is critical. These, along with regular security scans, will protect the system from cyber threats and unauthorized access. When it comes to the bus fleet, equipping vehicles with GPS tracking, installing CCTV cameras at depots, and restricting access with secure entry systems will go a long way in preventing theft and vandalism.

Depots and transit stops should be well-protected too, with measures like keycard or biometric access, 24/7 security cameras, and proper lighting to improve safety. Mobile apps used by passengers need secure encryption, MFA, and periodic security checks to keep them safe to use. Customer data must be encrypted, accessible only to authorized personnel, and securely deleted when no longer needed.

By focusing on these simplified recommendations, DART can address key vulnerabilities while ensuring efficient and secure operations. Regular reviews and updates to these measures will help DART stay ahead of potential threats.

Finally, physical security is key. Installing CCTV cameras, setting up alarm systems, and restricting access to sensitive areas like depots and server rooms will ensure that DART's operations remain safe and secure.

References

https://www.dartfirststate.com/
https://www.investopedia.com/terms/r/risk-analysis.asp