ISEC3080

Enterprise Security

Final Assignment

Jones,Christopher w0136969

2025-04-13

CONTENTS

Assignment Parameters

Preamble

Combine your assignments so far to create end-to-end secure enterprise system documentation. Your documentation, and presentation, will be supported by a prototype version of your system.

Final Proposal Document

Your final proposal document should be built using your original proposal and refined with feedback and your subsequent assignments. You should also provide details of your accompanying prototype system. The majority of the final is made from existing assignments; however, you should take this opportunity to refine and improve your previous work. Your final proposal should include the following sections:

Existing Sections

Summary
Overview & Objective
Timeline
Budget
Resources
Design
Implementation
Security
Policies and Procedures
Handover
Risks

New Sections

Change Management. Outline the structured process for managing changes to the system.
Testing Plan. Plan to validate operation and security of your system.
Prototype Overview. What aspects of your system you have implemented? What changes would be needed to take the prototype to the next level?

Presentation

As part of your final, you will need to deliver a presentation outlining your proposal and exhibit your prototype system. Your presentation should be between 10–15 minutes with an additional 5 minutes for questions. You presentation should provided an overview of your system, your three tiers and the security within your system. You should also provide a short demo using your prototype system.

Presenters will be chosen randomly on the first day of the presentation. Non-presenters are expected to attend and actively participate as the audience.

AeroShield Dynamics Inc.

About Us

Founded in Halifax, Nova Scotia, **AeroShield Dynamics Inc.** is a cutting-edge technology company specializing in the design, development, and manufacturing of advanced drones for emergency services. With a mission to enhance public safety, disaster response, and critical infrastructure protection, we provide reliable, high-performance unmanned aerial solutions for law enforcement, search and rescue teams, firefighting units, and medical transport services.

Our Mission

At AeroShield Dynamics, we are dedicated to revolutionizing aerial support for emergency response teams. Our drones are built to operate in high-risk environments, delivering real-time intelligence, aerial surveillance, and rapid deployment capabilities. By integrating AI-driven analytics, advanced sensors, and secure communication networks, we empower first responders with the tools they need to save lives and protect communities.

Our Expertise

- Emergency Response Drones: UAVs equipped with thermal imaging, LiDAR scanning, and AI-driven object detection to assist firefighters, police, and rescue teams.
- Medical Transport Drones: Unmanned aerial systems designed for rapid delivery of medical supplies, organs, and life-saving equipment in remote or disaster-affected areas.
- Industrial Inspection & Security: High-endurance drones tailored for critical infrastructure monitoring, border surveillance, and hazardous site inspections.

Our Facilities

Headquartered in Halifax, Nova Scotia, our state-of-the-art research, development, and manufacturing facility is equipped with advanced testing labs, precision engineering workshops, and a dedicated UAV flight-testing range. Strategically located near key maritime and aerospace hubs, we collaborate with government agencies, military partners, and private sector clients to push the boundaries of drone innovation.

Commitment to Innovation & Security

As a leader in aerial technology, AeroShield Dynamics prioritizes cybersecurity, regulatory compliance, and ethical AI integration in all our UAV systems. Our drones are built to withstand harsh environments, ensuring mission-critical performance for emergency responders.

With a vision to make aerial intelligence accessible, efficient, and secure, AeroShield Dynamics is shaping the future of drone technology for public safety and emergency management.

FINAL PROJECT REPORT

Secure 3-Tier Enterprise System for AeroShield Dynamics Inc.

Summary

This document presents the final consolidated proposal for the design, development, deployment, and secure implementation of a 3-tier enterprise system for AeroShield Dynamics Inc., a Halifax-based drone manufacturer specializing in emergency services. The system will facilitate secure and scalable management of inventory, production, employee administration, and client interaction. It integrates refined elements from previous assignments and reflects peer-reviewed feedback to ensure a professional-grade enterprise solution.

Overview & Objective

1.

AeroShield Dynamics Inc. aims to implement a 3-tier IT system architecture comprising Web, Application, and Database servers. The goal is to enhance operational efficiency, improve security posture, and support long-term scalability for its 500-employee operation. The solution must adhere to NIST SP 800-53 and OWASP ASVS security standards.

Statement of Work (SOW)

Scope:

- **Web server**: develop a web sever handle user access and provide a frontend interface for employees and clients.
- **Application Server:** Build an application server for business logic, including order processing, production monitoring, and integration with drone systems.
- **Database server**: Implement a database server to store critical data such as employee records, client details, inventory, and drone specifications.

Deliverables:

- A functional and secure 3-tier system accessible to authorized employees and clients.
- Scalable architecture to handle business growth and ensure high availability.
- A disaster recovery plan to protect critical business data.

Key Milestones:

- Requirements Gathering
- System Design
- Hardware and Software Procurement
- Development and Integration
- Testing and Quality Assurance
- Deployment and Training

Timeline

Phase	Duration	Tasks
Requirements Gathering	3 weeks	Stakeholder meetings, requirement specs
System Design	4 weeks	Architecture planning, tech selection
Procurement	2 weeks	Hardware/software acquisition
Development	8 weeks	Server config, application & DB development
Integration & Testing	6 weeks	QA testing, penetration testing
Deployment & Training	4 weeks	Go-live, staff onboarding

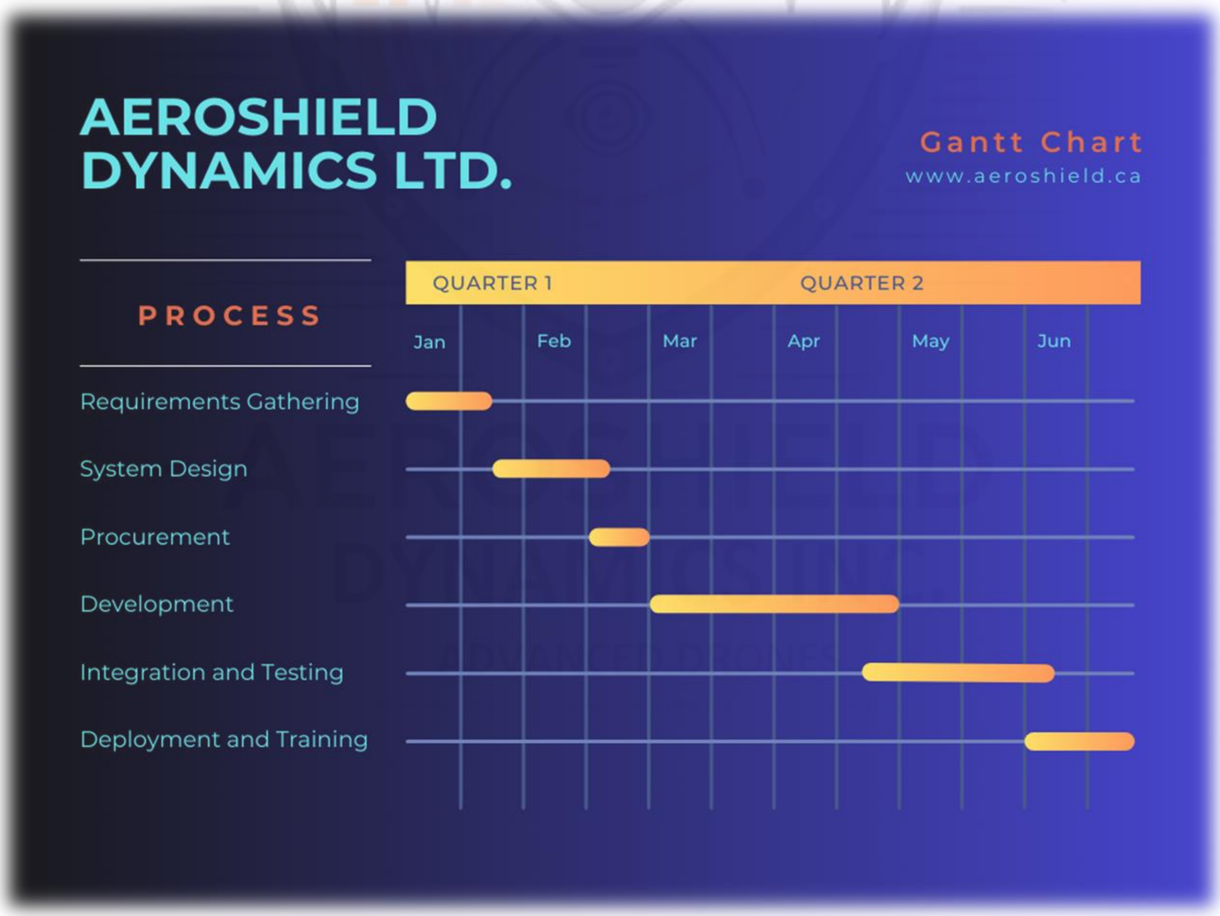

Figure 1 Timeline Gantt Chart

Budget

Estimated Budget **$2,155,000**

Category	**Cost**
Hardware/Infrastructure	$1,300,000
- On-premises servers (Web, App, DB)	$150,000
- Networking equipment & storage	$150,000
- 500 laptops	$500,000
- 500 cell phones	$500,000
Software	$300,000
- Licensing (OS, database, middleware)	$200,000
- Development tools & IDEs	$100,000
Labor (6 months)	$435,000
- Project Manager (1 full-time)	$90,000
- Software Engineer (1 full-time)	$75,000
- Senior Developers (2 full-time)	$120,000
- Software Developers (2 full-time)	$100,000
- Contractors/Consultants (as needed)	$50,000
Miscellaneous	$120,000
- Training and documentation	$20,000
- Contingency fund	$100,000
Estimated Budget Total	$2,155,000

Resources

Hardware:

- *Servers*: 3 server tiers: Web, Application, and Database.
- *Storage*: SAN storage with RAID 10 for redundancy.
- *Networking*: Enterprise-grade switches, routers, and firewalls.
- *Backup Systems*: Cloud or hybrid backup solution (Azure).

Software:

- *Web Server*: Apache
- *Application Server*: Middleware such as Node.js, Django, or ASP.NET.
- *Database Server*: MySQL, PostgreSQL, or Microsoft SQL Server.
- *Security Tools*: Endpoint protection, monitoring tools, and firewalls.

Personnel:

- *Project Manager*: Oversee timeline and deliverables.
- *Software Engineer*: Oversee system architecture.
- *Senior Software Developers (2)*: Supervise and work on more challenging development assignments.
- *Developers (2)*: Build and integrate application features.
- *System/Network Administrators (2)*: Configure servers, ensure security, and provide user support.
- *Contractors***:** External contractors as needed for vulnerability assessment, penetration testing, and quality control.

System Design

Web Server (Presentation Layer): Provides the frontend interface for employees and clients.

- React.js frontend with TLS encryption and WAF

App Server (Business Logic Layer): Processes business operations such as order management and production tracking.

- Node.js/Python backend with secure API gateway and RBAC

Database (Data Layer): Securely stores critical company data.

- PostgreSQL with AES-256 encryption and IDS

Security Measures at Each Tier

- Web Server Security: HTTPS, TLS Encryption, Web Application Firewall (WAF)
- Application Server Security: Secure API Gateway, Access Controls, Logging & Monitoring
- Database Server Security: Data Encryption, Role-Based Access Control (RBAC), Intrusion Detection System (IDS)
- Security Frameworks: Compliance with NIST SP 800-53 and OWASP ASVS for secure development

Architecture Diagram: Includes 3 tiers and associated security layers

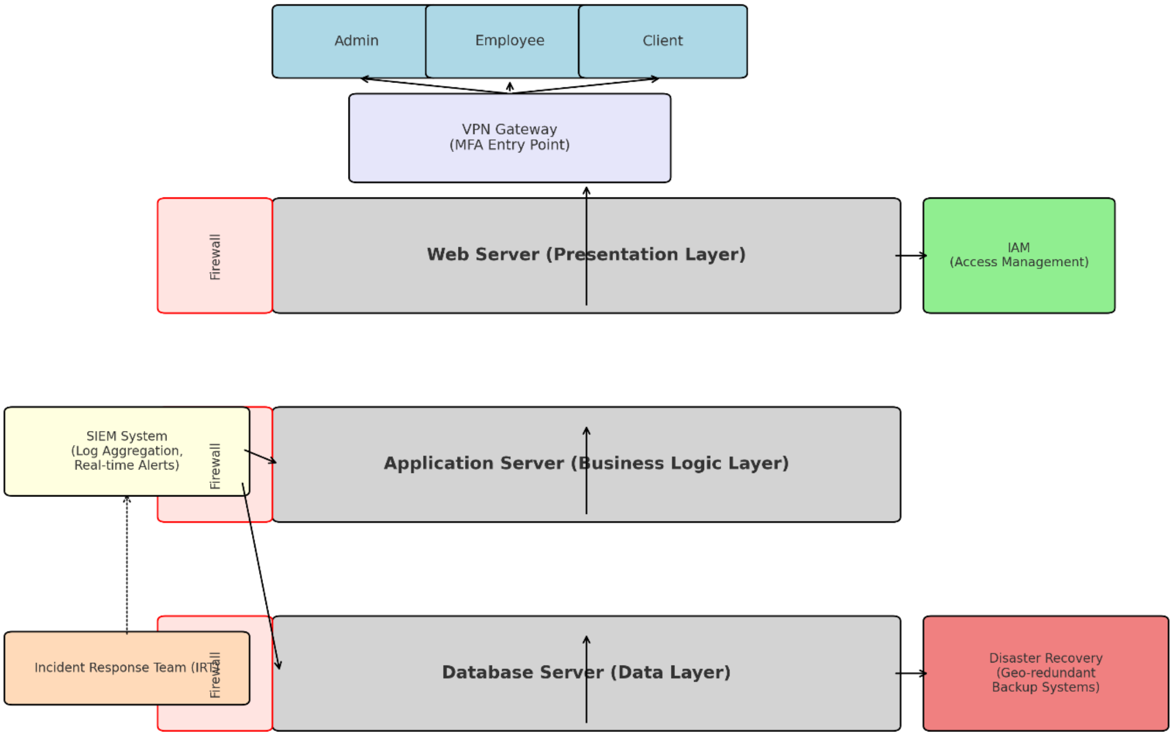

Figure 2 3-tier architecture diagram

Implementation

Technologies Used

- Frontend: React.js, HTML, CSS
- Backend: Node.js, Python (Django)
- Database: PostgreSQL with encryption
- Security: OAuth2, MFA, AES-256 Encryption, SIEM

Deployment Considerations

- Cloud-Based Infrastructure: Deployed on AWS EC2, RDS with IAM and MFA integration
- On-Premise Considerations: VPN, internal firewalls, and endpoint protection
- Physical & Cloud Backup Strategies: SAN storage with RAID 10 for redundancy and hybrid cloud backups (AWS/Azure)

Security

Authentication & Authorization

- OAuth2.0-based authentication with MFA
- Role-based access controls (RBAC)

Data Protection & Encryption

- Data at rest: AES-256 encryption
- Data in transit: TLS 1.3 encryption

Intrusion Detection & Monitoring

- Real-time logging with SIEM
- Automated alerts for suspicious activities

Compliance with Security Frameworks

- Adherence to NIST SP 800-53 for risk management and security controls
- Implementation of OWASP ASVS for secure application development

Policies and Procedures

Backup & Disaster Recovery

- Daily automatic backups with geo-redundancy
- Disaster recovery plan with Recovery Time Objective (RTO) of 2 hours
- Physical and Cloud Backup strategies for data resilience

Compliance & Regulatory Standards

- NIST SP 800-53 security framework compliance
- OWASP ASVS for secure application development

Security Risk Management & Response Plan

- Role-based access control enforcement
- Cybersecurity threat monitoring and incident response planning
- Regular penetration testing and security audits
- Contingency measures for emergency system failures

Handover

Knowledge Transfer

System Architecture & Security

- 3-Tier Enterprise Security System (Web Server, Application Server, Database Server)
- Security measures implemented at each layer, including encryption, access controls, and intrusion detection systems.
- Compliance with security frameworks (NIST SP 800-53, OWASP ASVS)

Project Implementation Details

- Development, integration, and deployment of enterprise security components.
- Technologies used (React.js, Node.js, PostgreSQL, AWS, VPN, SIEM, MFA, OAuth2).
- System monitoring and logging strategies.

Security Policies and Risk Management

- Cybersecurity threat monitoring and incident response procedures.
- Backup and disaster recovery plans (daily automatic backups, geo-redundancy, RTO of 2 hours).
- Risk assessment and mitigation strategies.

Personnel & Stakeholders

- Overview of team roles and responsibilities (Project Manager, Software Engineers, Developers, Network Administrators, Contractors).
- Key contacts for system support and security escalation procedures.

Ongoing Maintenance & Compliance

- Scheduled security audits, penetration testing, and compliance reviews.
- Documentation updates and regulatory adherence.

Handover Timeline and Responsibilities

Transition Schedule

Phase	Duration	Tasks & Responsibilities
Knowledge Transfer	2 weeks	Conduct walkthroughs, document system details, share security protocols.
Shadowing Period	3 weeks	Successor works alongside the current team to observe operations.
Gradual Handover	2 weeks	Successor takes over core responsibilities with supervision.
Independent Operation	3 weeks	Successor manages operations with periodic check-ins.
Final Review & Sign-Off	1 week	Address final queries, verify transition completion, obtain sign-off.

Roles & Responsibilities

- **Current Team**: Provide detailed documentation, walkthroughs, and hands-on training.
- **Successor**: Attend training, review documentation, ask clarifying questions, and demonstrate competence in assigned tasks.
- **Management**: Oversee the transition, ensure continuity, and address escalations.

Communication Plan

Key Stakeholders & Communication Methods

Stakeholder	**Communication Channel**	**Frequency**
Transition Team	Scrum meetings, email updates	Weekly
IT & Security Teams	Security briefings, documentation handover	Bi-Weekly
Management	Progress reports, risk assessments	Monthly
End-Users & Clients	User training, support documentation	As needed

Transition Documentation

- **System Documentation**: Architectural diagrams, security configurations, access controls.
- **Process Guidelines**: Standard operating procedures (SOPs) for security monitoring, incident response, and compliance audits.
- **Training Materials**: User guides, walkthroughs, video tutorials for system operations.
- **FAQs & Troubleshooting Guides**: Common issues, resolution steps, and escalation contacts.

This structured transition plan ensures continuity, security, and minimal disruption during the handover process.

Risk Management Plan

Introduction

This Risk Management Plan aims to identify, assess, and mitigate key risks associated with the transition-out process and ongoing operations of the 3-Tier Enterprise Security System. The plan ensures that risks are proactively managed to minimize disruptions, maintain security compliance, and ensure business continuity.

Risk Identification & Analysis

The following risks have been identified as potential threats to the transition-out process and overall system security:

Risk 1: Data Loss or Corruption During Handover

- Likelihood: High
- Impact: Critical
- Description: Data loss or corruption could occur during system transition due to improper backups, human error, or cyber threats. This could lead to system downtime and loss of critical enterprise information.
- Mitigation Strategy:
  - Implement a robust backup and disaster recovery plan with automated daily backups and geo-redundancy.
  - Conduct verification testing before transferring data.
  - Establish a rollback plan to restore data in case of corruption.
  - Use encryption (AES-256) and secure transmission protocols (TLS 1.3) for data transfer.

Risk 2: Cybersecurity Threats and Unauthorized Access

- Likelihood: Medium
- Impact: High
- Description: During the transition, there is an increased risk of cyber threats such as unauthorized access, data breaches, or insider threats due to changing access controls and oversight gaps.
- Mitigation Strategy:
    - Implement strict Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) for all user accounts.
    - Conduct penetration testing before and after transition to identify vulnerabilities.
    - Maintain real-time monitoring through Security Information and Event Management (SIEM).
    - Update security policies and enforce compliance with NIST SP 800-53 and OWASP ASVS frameworks.

Risk 3: Lack of Knowledge Transfer Leading to Operational Disruptions

- Likelihood: High
- Impact: Moderate
- Description: Inefficient knowledge transfer may lead to operational gaps, impacting system performance, troubleshooting, and security monitoring after the transition.
- Mitigation Strategy:
    - Conduct structured training sessions for successors, including technical walkthroughs and documentation reviews.
    - Provide shadowing opportunities where the new team can work alongside the outgoing personnel.
    - Create a comprehensive knowledge base with FAQs, troubleshooting guides, security policies, and compliance procedures.
    - Schedule follow-up assessments post-transition to ensure effective knowledge retention.

3. Risk Monitoring & Review

To ensure continuous risk management, the following monitoring and review actions will be taken:

Risk	Monitoring Strategy	Review Frequency
Data Loss	Backup integrity checks, system audits	Weekly
Cybersecurity Threats	Security event logging, intrusion detection	Continuous monitoring
Knowledge Transfer	Training effectiveness assessment	Monthly

4. Contingency Planning

- Emergency Response Protocols: Clearly defined response procedures for data recovery, cybersecurity breaches, and access control issues.
- Incident Response Team (IRT): Designated team responsible for handling high-risk incidents and minimizing impact.
- Regular Testing & Drills: Conduct cybersecurity simulations, disaster recovery drills, and role-based access control evaluations.

5. Conclusion

By implementing this Risk Management Plan, the transition-out process will be safeguarded against potential threats, ensuring a seamless handover with minimal disruption. Proactive risk monitoring, structured training, and robust cybersecurity measures will help maintain the integrity and security of the 3-Tier Enterprise Security System.

Change Management

To ensure stability, compliance, and minimal disruption, AeroShield Dynamics Inc. will implement a formal Change Management Process guided by ITIL best practices. The objective is to manage and communicate changes effectively across the system lifecycle.

1. Change Request Initiation

- Change Requests (CRs) are submitted using a standardized form via the internal IT Service Management (ITSM) portal.
- All CRs must include:
  - Business justification
  - Impact analysis
  - Rollback plan
  - Testing requirements

2. Change Categorization

- **Standard Changes**: Pre-approved, low-risk, recurring changes (e.g., patching).
- **Emergency Changes**: Unplanned but urgent changes required to resolve incidents (e.g., zero-day vulnerabilities).
- **Major Changes**: High-risk or large-impact changes requiring in-depth review (e.g., server migrations, architecture updates).

3. Review and Approval

- Weekly Change Advisory Board (CAB) meetings to review and approve CRs.
- Emergency changes may be approved by senior IT leadership and reviewed retroactively by the CAB.

4. Pre-Implementation

- All changes undergo:
  - Impact assessment
  - Security review
  - Testing in a staging environment
  - User communication and scheduling

5. Implementation & Rollback

- Implemented during pre-approved windows.
- Documented **rollback procedures** in place for failed changes to restore prior state rapidly.

6. Post-Implementation Review

- Completed changes are reviewed to:
  - Assess success/failure
  - Identify lessons learned
  - Update documentation accordingly

7. Change Logging & Documentation

- All changes will be logged in the ITSM system with timestamps, approvers, rollback results, and related test results to maintain accountability and support future audits.

Testing Plan

To validate functionality, integration, and security of the 3-tier system, a comprehensive multi-stage testing strategy will be employed throughout development and deployment.

1. Functional Testing

- Unit testing of frontend, backend, and database modules
- Conducted using Jest (React), PyTest (Django), and SQL scripts
- Test Cases:
    - Login/logout
    - User role assignment
    - Inventory update workflows

2. Integration Testing

- Validate interactions across tiers (Web ↔ App ↔ DB)
- Use of Postman, Selenium, and custom test harnesses
- Scenarios include order processing, drone telemetry integration, and user CRUD operations

3. Performance Testing

- Simulated load tests using Apache JMeter or Locust
- Key metrics:
    - Response time (max: 2s)
    - Concurrent users (target: 1000+)
    - System throughput (TPS)

4. Security Testing

- Penetration testing by 3rd-party contractor
- Vulnerability scanning with Nessus and OWASP ZAP
- Test for:
  - SQL injection
  - CSRF/XSS
  - Insecure deserialization
  - Authentication bypass

5. User Acceptance Testing (UAT)

- Involve 10–15 employees from key departments
- Validate real-world workflows and ease of use
- UAT feedback loop to development team for refinements

6. Continuous Testing Pipeline

- CI/CD pipeline includes automated regression tests via GitHub Actions
- Security checks with Snyk or SonarQube before deployments

Prototype Overview

A working prototype was developed to demonstrate the core architecture and functionality of the proposed 3-tier enterprise system. This prototype demonstrates feasibility of secure access control and layered architecture, ensuring project viability before full-scale investment.

1. Prototype Components Implemented

Frontend (Web Tier):

- React.js-based login portal
- Role-specific dashboards for admin and employee users
- TLS encryption via self-signed certificates

Backend (Application Tier):

- Node.js server with Express.js RESTful API
- Business logic for login, role-based access, and basic inventory queries
- OAuth2 authentication and MFA using Google Authenticator

Database (Data Tier):

- PostgreSQL database with AES-256 data encryption
- Sample data set including employee records and mock drone inventory
- Stored procedures for data access abstraction

2. Security Features

- MFA and OAuth2.0 login flows
- TLS 1.3 encryption for all data in transit
- Role-Based Access Control (RBAC) with logging

3. Limitations

- Prototype runs on localhost / development environment
- Scaled for 10–20 test users only
- Does not include real-time telemetry integration or enterprise-wide deployment tools

4. Next Steps Toward Production

- Deploy on AWS infrastructure using EC2 and RDS with IAM roles
- Implement full integration with drone telemetry systems and real-time processing
- Expand user management features and auditing
- Migrate to centralized identity management (e.g., Azure AD)

Conclusion

This project has successfully demonstrated the feasibility and design of a secure 3-tier enterprise system for AeroShield Dynamics Inc. Through structured change management, rigorous testing, and a security-first design approach, the organization is well-positioned to move forward with full-scale implementation and production deployment. Future efforts will focus on scaling, cloud deployment, and telemetry integration to support evolving operational needs.

References

- Assignment 1: Project Plan
- Assignment 2: RFP
- Assignment 3: Prototype Technical Guide
- Assignment 4: Transition and Risk Management Plan
- Company Background Document (unsubmitted)