Information Security Audit Report: ABC Air

Module: Secure Design and Development
Student Name: John Brown
Student ID: 1234567
Date: October 14, 2024

Table of Contents

Introduction

ABC Air is a small aircraft service company that carries out aircraft maintenance for civil operators. The company records flying hours, servicing time, and man-hours of engineers. Recently, an external contractor provided a report outlining a solution using a web-based system. The system was developed using the Flask framework and deployed on PythonAnywhere.

The purpose of this report is to perform an information security audit on the provided documentation for the ABC Air system. This report will identify a suitable audit approach, perform a security audit of the system based on the provided technical details, and critically evaluate the frameworks used. The audit will focus on the confidentiality, integrity, and availability (CIA) of the data managed by the system, such as aircraft logs and engineer details.

Section 1: Identification & Adoption of Standards

2.1 Audit Approach

For the audit of ABC Air, I have selected a **Control-based approach**. This approach focuses on checking if specific security controls are in place and if they are working as intended. This is suitable for ABC Air because they have a specific set of requirements and a new system that needs to be checked against best practices. A risk-based approach could also be used, but since the system is already built, checking the controls is more direct.

The audit will assess the system against international standards to ensure that the aircraft maintenance data is secure. Since ABC Air deals with civil aviation data, integrity is very important.

2.2 Selected Frameworks

The following standards and frameworks have been identified as relevant for this audit:

1. ISO/IEC 27001
ISO 27001 is the international standard for Information Security Management Systems (ISMS). It provides a checklist of controls that organizations should implement to keep information assets secure (ISO, n.d.). For ABC Air, this standard is useful because it covers all aspects of security, including access control and physical security. It ensures that the company follows a recognized standard which is good for their reputation.
2. COBIT (Control Objectives for Information and Related Technologies)
COBIT is a framework for IT governance and management. It helps organizations generate value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. For ABC Air, COBIT can help in aligning their IT goals with their business goals, ensuring that the Flask application supports the maintenance work effectively.
3. OWASP (Open Web Application Security Project)
Since the system is a web application built with Flask, OWASP guidelines are very important. The OWASP Top 10 lists the most critical security risks to web applications. This framework will be used to check if the specific code and design of the ABC Air app are secure against common attacks like SQL Injection and Cross-Site Scripting (XSS).

Section 2: Information Security Audit & Assurance

This section outlines the findings of the audit performed on the ABC Air system documentation, specifically pages 5 to 21 of the brief.

3.1 Technical Audit Findings

Based on the review of the "Strengths and Limitations" table and the system design provided in the brief, several issues were identified.

Input Validation and Sanitation
The documentation states that the system has "Input validation" which is a strength. For example, the registration page checks if an email is valid. However, the limitation section admits there is "No input sanitation". This is a significant finding. Input sanitation is crucial to

prevent malicious code from being entered into the database. Without sanitation, the system is vulnerable to attacks where hackers input scripts into forms.

Authentication and Password Security

The system uses Flask-Bcrypt to hash passwords, which is a good security practice. This ensures that if the database is stolen, the passwords are not readable. However, a major weakness identified is the lack of "Two-Factor Authentication (2FA)". In modern security, relying only on a password is not enough, especially for admins who can delete aircraft data. The brief explicitly states "No 2FA" as a limitation.

Session Management

The system uses Flask-Login for session management. This is a standard library, which is good. However, the brief mentions that the system supports "multiple simultaneously logged in users". While this is a feature, it can be a risk if an admin logs in on a public computer and forgets to log out, and then logs in somewhere else. The session might remain active.

Deployment Environment

The system is deployed on PythonAnywhere. The brief quotes PythonAnywhere support saying that "each user can see only the files in their own section of the disk". This suggests the hosting is relatively secure. However, the system relies on a shared hosting environment, which might have limitations regarding performance if traffic spikes, though for a small company like ABC Air, this might be acceptable.

3.2 Risk Assessment

Using a qualitative risk assessment matrix, the following risks have been identified for ABC Air:

Risk Description	**Likelihood**	**Impact**	**Risk Level**	**Mitigation**
SQL Injection	High	High	**Critical**	The system uses SQLAlchemy which helps, but the lack of input sanitation mentioned in the brief is a worry. Attackers could manipulate the database.
Unauthorized	Medium	High	**High**	Because there

Access				is no 2FA, if an admin password is guessed (e.g., "123456" as seen in the test screenshots), an attacker can delete all data.
Data Loss	Low	High	**Medium**	The brief mentions the ability to "Delete Aircraft" and "Delete Engineer". If this is done accidentally by an admin, there is no mention of a backup or recovery feature.
Insider Threat	Medium	Medium	**Medium**	Engineers might try to access admin privileges. The system adheres to the "Principle of Least Privilege" which mitigates this, but internal staff are always a risk.

The most critical risk is the potential for SQL injection or similar injection attacks due to the explicit lack of sanitation mentioned in the documentation limitations.

3.3 GDPR Compliance

The provided GDPR Compliance Test image (Figure 18 in the brief) shows some concerning results.

- **Privacy Policy:** The test result shows "Privacy Policy was not found". For a company operating in the UK/EU, this is a violation of GDPR. Users (engineers) need to know how their data is used.
- **Cookie Protection:** The test says "No cookies with personal information seem to be sent", which is good.
- **TLS Encryption:** The site uses HTTPS, which is good configuration.

Overall, the system is partially compliant but fails on the documentation side regarding Privacy Policies.

Section 3: Critical Evaluation of Frameworks

This section evaluates the benefits and limitations of using frameworks like ISO 27001 and COBIT for a company like ABC Air.

4.1 Benefits of Standards

Using standards like **ISO 27001** has many benefits. Firstly, it provides a comprehensive framework. It ensures that nothing is missed. For ABC Air, this means they don't just focus on the software but also on people and physical security. According to Klipper (2015), ISO 27001 helps in managing risks systematically.

COBIT is beneficial because it aligns IT with business. ABC Air needs their aircraft maintenance logs to be accurate for their business to function. COBIT ensures that the IT controls support this business goal. It provides a common language for management and IT professionals.

OWASP is essential for the web application. It is specific to software development. The benefit is that it provides concrete technical checks (like checking for Injection flaws) that high-level standards like ISO might miss.

4.2 Limitations

However, there are limitations to these frameworks.
Complexity and Cost: ISO 27001 is very complex. It has hundreds of controls. For a small company like ABC Air, implementing the full standard would be very expensive and time-consuming. They might need to hire a dedicated security officer, which they might not

afford. As noted by some sources, small businesses often struggle with the paperwork required by ISO.
Rigidity: Frameworks can sometimes be too rigid. COBIT can be seen as bureaucratic. ABC Air is a small agile company; they might find the heavy documentation required by COBIT slows them down. The "Waterfall model" used in the development is already rigid, and adding heavy governance might make it worse.

Not a Silver Bullet: Just because a company has ISO 27001 certification doesn't mean they are 100% secure. They can still be hacked. The standard is about managing risk, not eliminating it.

In conclusion, while frameworks provide a good structure, they need to be adapted for a Small-to-Medium Enterprise (SME) like ABC Air to avoid being a burden.

Conclusion

The audit of the ABC Air information security system has highlighted both strengths and weaknesses. The use of Flask and PythonAnywhere provides a functional base, and the use of HTTPS and password hashing shows some awareness of security. However, significant gaps exist, particularly the lack of input sanitation, the absence of Two-Factor Authentication (2FA), and the missing Privacy Policy for GDPR compliance.

The audit approach chosen was control-based, using standards like ISO 27001 and OWASP. These frameworks are useful for identifying what is missing. However, as discussed in the critical evaluation, they must be applied carefully to avoid overwhelming the small company with bureaucracy.

It is recommended that ABC Air immediately implements 2FA for admin accounts and adds a proper Privacy Policy to the website. They should also perform a code review to ensure input sanitation is implemented despite the limitations stated in the brief.

References

Coventry University. (2024). *Assignment Brief: Secure Design and Development*.

ISO. (n.d.). *ISO/IEC 27001 Information security management*. Available at: https://www.iso.org/isoiec-27001-information-security.html

Klipper, L. (2015). *Information Security Risk Management*. Syngress.

OWASP. (2021). *OWASP Top 10*. Available at: https://owasp.org/www-project-top-ten/

PythonAnywhere. (2015). *Data security and general PythonAnywhere queries*.

Immersives. (n.d.). *Flask-Login documentation*.