Module 5 – Cybersecurity Governance, Risk Management, and Operational Compliance in Airport Operations

Module 5

Cybersecurity Governance, Risk Management, and Operational Compliance in Airport Operations

This module marks a shift towards a deep dive into the practical implementation of cybersecurity within airport operations. Building on foundational knowledge of airport administration and its initial links to cybersecurity from previous modules, Week 5 focuses on how to actively establish and maintain a robust cybersecurity posture. We will explore the operationalization of cybersecurity governance frameworks, the hands-on execution of comprehensive risk management processes tailored for airport environments, and the critical steps for ensuring ongoing compliance with key regulatory directives and industry standards. The emphasis will be on translating cybersecurity theory into actionable practices, utilizing specific tools, techniques, and official guidance to secure airport administrative and operational systems.

Lecture Focus

The lecture will concentrate on several key areas of practical application, including the operationalization of airport cybersecurity governance, the techniques for practically applying cybersecurity risk management to diverse airport administrative and operational systems, the methods for meeting critical cybersecurity compliance mandates such as TSA directives, and a detailed exploration of implementing cybersecurity frameworks like the NIST CSF within an airport context.

Cybersecurity Focus

Our cybersecurity focus this module will be on the practical steps involved in developing and enforcing effective airport-specific policies, conducting thorough airport-focused risk assessments, and operationalizing key TSA directives. Further, we will delve into implementing robust procedures for the protection of Sensitive Security Information (SSI), the necessary preparations for undergoing cybersecurity audits, and the detailed, step-by-

step application of the NIST Cybersecurity Framework to enhance overall airport security posture.

Course Outcomes & Objectives Alignment

- **Outcome 1:** Demonstrate an understanding of the cybersecurity measures necessary to protect stakeholder data and ensure secure communication in airport administration.
    - **Objective 1.1:** Recall basic data integrity and availability principles (through practical risk assessment of administrative and operational data).
    - **Objective 1.2:** Describe the importance of secure communication between airport stakeholders and its role in protecting sensitive information (through policy development for SSI and vendor communications).
    - **Objective 1.4:** Analyze stakeholder communication systems to determine vulnerabilities and propose methods for securing sensitive exchanges (addressed through threat modeling, policy development, and implementing security for governance/legal data).
    - **Objective 1.5:** Design an access control system using role-based access to ensure that only authorized personnel can modify sensitive administrative and stakeholder data (through implementing TSA access control directives and CSF Protect functions).
- **Outcome 3:** Analyze the role of governance structures in implementing cybersecurity practices that comply with federal regulations and protect airport management systems.
    - **Objective 3.1:** Identify key federal regulations that guide airport cybersecurity practices (through deep dive into implementing TSA & FAA directives).
    - **Objective 3.2:** Understand the role of governance

structures in enforcing cybersecurity policies within airports (through operationalizing governance and aligning leadership with cyber strategy).
    - **Objective 3.3:** Evaluate compliance with cybersecurity regulations by conducting periodic audits to ensure adherence to FAA and TSA standards (through practical audit preparation and techniques).
    - **Objective 3.4:** Create strategies to secure governance and legal data related to airport sponsor agreements (through implementing SSI protection and risk management for legal/contractual data).
    - **Objective 3.5:** Monitor and adapt cybersecurity practices to stay aligned with updates to federal and state regulations (through continuous improvement processes inherent in CSF and audit feedback mechanisms).
- **Outcome 4:** Apply cybersecurity protocols to protect financial management systems, ensuring compliance with federal policies and preventing unauthorized access to sensitive financial data.
    - **Objective 4.1:** Recall the basic principles of PCI-DSS and their importance in securing financial transactions (applied when discussing financial system risks and compliance during risk assessments and policy development).
- **Outcome 5:** Evaluate cybersecurity risks in airport commercial development and property management, applying solutions to safeguard digital systems and tenant data.
    - **Objective 5.1:** Recall the importance of encryption in securing tenant and contractor data during commercial transactions (as part of implementing overall data protection policies and vendor management).
    - **Objective 5.2:** Understand the relationship between cybersecurity measures and the protection of airport

property management systems (through asset identification and risk assessment for these systems).
    - **Objective 5.3:** Assess tenant and contractor data protection measures to ensure compliance with airport cybersecurity protocols (via vendor risk management techniques and contractual cybersecurity requirements).
- **Outcome 6:** Assess the cybersecurity considerations in managing the Airport Improvement Program (AIP) and capital development funding processes to prevent cyber threats and ensure data integrity.
    - **Objective 6.2:** Explain the role of vendor cybersecurity practices in ensuring the security of capital development projects (through third-party risk management section in governance).
    - **Objective 6.4:** Evaluate the cybersecurity practices of vendors and contractors to mitigate third-party risks (through third-party risk management section in governance).

CM Module Content

- **CM Module 1:** Finance and Administration of Airports (Sections: The Regulated Airport; Airport Financial Management; Airport Business Operations - for context on governance, compliance drivers, financial/procurement systems requiring security).
- **CM Module 2:** Planning, Construction & Environmental (Section: Airport Planning - for context on data assets like ALPs/Master Plans that need protection).
- **CM Module 3:** Airport Operations, Security and Maintenance (Section: Airport Security - for context on existing security frameworks like the ASP, and systems like PACS that need cybersecurity layers).

Module 5 – Overview
Web Page

Module 5 – Reading
Web Page

Module 5 - Presentation
PDF document

Module 5 – Podcast
Audio

Module 5 – Supplemental Websites and Videos
Web Page

Reading Material

DHS – Transportation Systems Sector Cybersecurity Framework Implementation Guidance
PDF document

DHS – NIPP 2013 Partnering for Critical Infrastructure Security and Resilience

PDF document

SSA PARAS – Quick Guide for Airport Cybersecurity

PDF document

GAO – Report 25-107947 – TSA Is Taking Steps to Enhance Cybersecurity, but Additional Actions Are Needed

PDF document

ICAO – FAA Cyber Strategy and Interagency Coordination Mechanisms

PDF document

TSA – 2018 Cybersecurity Roadmap

PDF document

ICAO – Cybersecurity Culture in Civil Aviation

PDF document

ICAO – Cybersecurity Policy Guidance

PDF document

ICAO – Cyber Information Sharing

PDF document

ICAO – Cybersecurity Action Plan – Second Edition

PDF document

ICAO – Aviation Cybersecurity Strategy

PDF document

ICAO – Compilation of Cyber Regulations

PDF document

Graded Assignments

Module 5 – In-Class Discussion

Assignment

[Broken Topic]

Assignment

Module 5 – Quiz

Quiz

Due Aug 19, 2025 11:59 PM