CSAAP

Course One

Introduction to Cybersecurity and Airport Administration

Module Five

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

Practical implement and establishment of robust cybersecurity infrastructure and processes in airport environments.

Sponsored by the US National Science Foundation

Cuyahoga Community College

Agenda

- Operationalizing Airport Cybersecurity Governance
- Aligning Leadership, Crafting Policies, Managing Vendor Risk
- Practical Cybersecurity Risk Management for Airport Systems
- Asset Identification, Threat Modeling, Risk Treatment
- Meeting Cybersecurity Compliance Mandates
- Implementing TSA Directives, Protecting SSI, Conducting Audits
- Framework Implementation Deep Dive: Applying NIST CSF

Objectives

- Implement strategies to align airport leadership with cyber strategy.
- Develop and enforce airport-specific cybersecurity policies using recognized guidance.
- Establish and manage a third-party/vendor cybersecurity risk management program.
- Conduct practical, airport-focused cybersecurity risk assessments.
- Translate TSA Cybersecurity Directives into actionable operational procedures.
- Apply procedures for protecting Sensitive Security Information (SSI).
- Outline the process for preparing for and conducting cybersecurity compliance audits.
- Apply the core functions of the NIST Cybersecurity Framework (CSF) to airport environments.

Operationalizing Cybersecurity Governance

- **Operationalized Governance**
  - *Moving beyond written policies to an active, integrated system of cybersecurity leadership, accountability, and decision-making.*
  - *Ensuring cybersecurity is a continuous process embedded in all airport administrative and operational functions.*

Operationalizing Cybersecurity Governance (Cont'd)

- **The Importance of Operationalized Governance**
  - *Provides strategic direction and ensures alignment of cybersecurity efforts with airport mission and risk appetite (building on airport administration fundamentals).*
  - *Establishes clear accountability for protecting critical airport systems (IT & OT), sensitive data (SSI, PII, financial), and ensuring operational continuity.*
  - *Drives compliance with complex regulatory landscapes (TSA Directives, FAA requirements, data privacy laws).*
  - *Fosters stakeholder trust (passengers, airlines, tenants, community) by demonstrating a commitment to security.*
  - *Enhances resource allocation and justifies cybersecurity investments.*

Operationalizing Cybersecurity Governance (Cont'd)

- **Key Actors in Airport Cybersecurity Governance:**
  - ***Airport Sponsor/Board:*** *Ultimate oversight, sets risk tolerance, approves major policies & budgets.*
  - ***Airport Executive (Director/CEO):*** *Primary champion, ensures strategy execution, accountable to the Sponsor.*
  - ***CISO/IT Security Lead:*** *Develops security strategy, oversees policy implementation, manages security operations and incident response.*
  - ***Department Heads (Operations, Finance, HR, Legal, etc.):*** *Implement policies within their domains, manage departmental cyber risks.*
  - ***All Employees & Contractors:*** *Adherence to policies, security awareness, reporting incidents (as emphasized by ICAO – Cybersecurity Culture in Civil Aviation).*
  - ***Regulatory Bodies (e.g., TSA, FAA):*** *Set baseline requirements and conduct oversight.*

Governance: Leadership and Buy-In

- **Engaging Top Airport Leadership:**
  - *Present a compelling business case for cybersecurity*
  - *Articulate cyber risks in terms of impacts on airport safety & compliance*
  - *Champion cybersecurity as an integral airport priority*
- **Who Owns Cyber Risk?**
  - *Define and secure executive agreement roles, responsibilities, and accountability*
  - *Establish regular reporting mechanisms to leadership, ensuring they remain informed, engaged, and can provide effective oversight.*
- **Cultivating Buy-in Across Key Airport Departments:**
  - *Articulate the value proposition of cybersecurity to each department*
  - *Actively involve department heads and key stakeholders (shared responsibility and governance).*

Governance: Frameworks & Regulatory Structures

- **Implement a Risk Assessment & Management Framework:**
  - *Establish a continuous cycle of identifying critical assets, assessing specific cyber threats and vulnerabilities, analyzing impact, and prioritizing risks.*
  - *Define airport-wide risk tolerance levels in collaboration with leadership.*
- **Develop Actionable Policies & Procedures:**
  - *Use resources like ICAO – Cybersecurity Policy Guidance to establish clear, practical, and enforceable cybersecurity policies.*
  - *Ensure policies comprehensively cover key areas like data protection (PII, SSI), access, reporting, etc. for all personnel, contractors, and relevant third parties.*
- **Structure for Regulatory Compliance:**
  - *Create a systematic approach to operationalize requirements regulators.*
  - *Assign clear ownership for compliance areas within departments.*

Governance: Continuous Improvement

- **Foster Shared Responsibility & a Strong Security Culture**
  - *Emphasize that cybersecurity is a collective responsibility across all airport departments, including IT, Operations, Security, Maintenance, and Administration.*
  - *Establish channels for all personnel to report threats and incidents.*
- **Implement Comprehensive Employee Awareness & Training**
  - *Deliver regular, engaging, and role-specific cybersecurity training that covers phishing, social engineering, password hygiene, secure data handling, and incident reporting procedures.*
  - *Utilize tools like phishing simulations to test and improve awareness.*
- **Develop & Test the Cyber Incident Response Plan (CIRP)**
  - *Create a Cyber Incident Response Plan that outlines procedures events and scenarios.*
  - *Regularly test the CIRP through drills and exercises.*

Governance: People, Posture, and Structure

- **Strategically Use Cybersecurity Technology & Tools**
  - *Deploy and manage appropriate technologies such as firewalls, IDS/IPS, SIEM systems, and Endpoint Detection & Response (EDR) tools.*
  - *Ensure these tools are configured according to established airport policies, are regularly updated, and that their outputs are actively monitored.*
- **Drive Continuous Monitoring & Improvement**
  - *Regularly assess the effectiveness of implemented cybersecurity controls through comprehensive security audits, vulnerability assessments, and penetration testing.*
  - *Integrate all findings directly into the airport's risk management process.*
- **Foster Collaboration & Information Sharing**
  - *Actively participate in aviation sector information sharing bodies, such as the Aviation ISAC, and maintain strong liaison with government security agencies.*

Governance: Compliance Mandates

- Understanding TSA's Role & Authority
  - *TSA Security Directives (SDs) and Emergency Amendments (EAs) – Mandatory Requirements. Focus of recent directives: Critical Infrastructure (Airports & Aircraft Operators).*
- Operationalizing Key TSA Cybersecurity Directive Requirements
  - ***Action:*** *Implementing Network Segmentation plans for IT and critical operational systems (e.g., PACS, BHS). Enforcing robust Access Control measures (MFA, least privilege) for identified critical systems.*
  - ***Process:*** *Establishing comprehensive Vulnerability Management & Timely Patching programs.*
  - ***Plan:*** *Developing and regularly testing Cyber Incident Response Plans per TSA specifications.*

Governance: Compliance Mandates (Cont'd)

- Adhere to FAA Cybersecurity Expectations and understand how grant assurances for airport improvement projects can include cybersecurity resiliency and data protection requirements.
- Operationalize 49 CFR Part 1520 for Protecting Sensitive Security Information (SSI) through stringent marking, handling, storage (physical and digital), and destruction procedures for documents like the Airport Security Program (ASP) and vulnerability assessments.
- Ensure Payment Card Industry Data Security Standard (PCI-DSS) compliance for all airport systems processing, storing, or transmitting cardholder data, such as those used for parking, concessions, and other revenue-generating streams.
- Prepare for and conduct regular Internal and External Cybersecurity Audits by developing audit plans, collecting evidence of control effectiveness, and using findings to drive remediation and continuous improvement of the airport's security posture.

Governance: Decision Frameworks

- **Action:** Formally Chartering the Airport Cybersecurity Program: Documenting scope, objectives, and authority.
- **Structure:** Defining a Cybersecurity Steering Committee or Governance Board – Composition (with key actors), meetings, and responsibilities.
- **Process:** Establishing clear, documented decision-making processes for:
  - *Cybersecurity investments and resource prioritization.*
  - *Policy exception requests and approvals.*
  - *Formal risk acceptance by appropriate leadership levels.*
- **Tool:** Utilizing a portion of the Airport Cybersecurity Program Plan to explicitly document this governance structure, roles, and decision rights (as guided by ACRP Report 140).

Risk-Based Governance in Airports

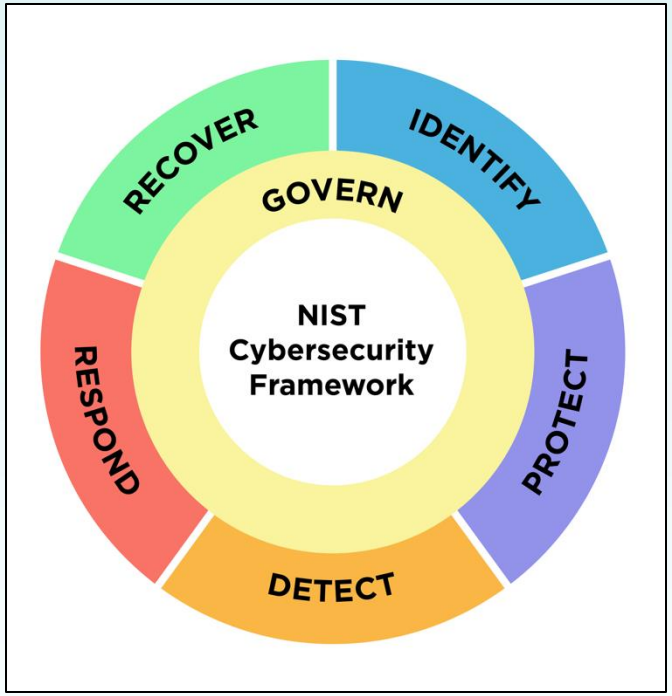
- Airports are complex environments with numerous interconnected IT and OT systems vital for safety, security, and operational efficiency.
- **Risk Identification and Treatment:**
  - *Proactively identifying, analyzing, and treating cybersecurity risks helps protect critical airport assets, ensure operational resilience, meet stringent regulatory obligations (like TSA Directives), and make informed, defensible decisions about security investments .*
- A structured risk management process enables airport leadership to understand and prioritize threats based on potential impact to the airport's mission

NIST CSF in Airports

- The NIST Cybersecurity Framework (CSF) provides a voluntary, yet widely adopted and highly recommended, high-level strategic framework for organizations, including airports, to assess and improve their ability to prevent, detect, and respond to cyber-attacks.
- It offers a common language and a structured approach for organizing diverse cybersecurity activities, helping airports to identify gaps, prioritize actions, and communicate their cybersecurity posture to stakeholders.
- For airports, the CSF helps translate broad cybersecurity goals into manageable and actionable categories, facilitating a comprehensive approach to protecting both administrative and operational systems.

Implementing NIST CSF

- Adopt NIST CSF for a common language and comprehensive structure to manage airport cybersecurity risk.
- Utilize CSF's five core Functions: Identify, Protect, Detect, Respond, Recover, to organize all airport cybersecurity activities.
- Leverage CSF to assess your airport's current posture, pinpoint gaps, prioritize crucial improvements, and effectively communicate security status.
- Customize CSF implementation to fit your airport’s unique size, operational complexity, and specific risk environment.



NIST CSF: IDENTIFY Function: Knowing Your Airport's Cyber Landscape

- **Asset Management (ID.AM):** Inventory and classify critical airport IT & OT systems (e.g., financial platforms, ALPs, PACS, BHS, airfield lighting) and vital data.
- **Governance (ID.GV):** Integrate cybersecurity roles, policy oversight, and risk approval processes into existing airport governance structures.
- **Risk Assessment (ID.RA):** Conduct regular, airport-specific cyber risk assessments targeting key systems and operational processes.
- **Risk Management Strategy (ID.RM):** Define and communicate the airport's strategy for managing identified risks, including leadership-approved risk tolerance levels.
- **Supply Chain Risk Management (ID.SC):** Implement processes to identify and assess cybersecurity risks from critical third-party vendors and service providers.

NIST CSF: PROTECT Function: Safeguarding Airport Assets & Operations

- **Access Control (PR.AC):** Enforce strong authentication (MFA) and least privilege principles for all user and system access to airport IT and OT networks, aligning with relevant TSA directives.
- **Awareness & Training (PR.AT):** Deliver continuous, role-specific cybersecurity training for all airport personnel on topics like phishing, secure data handling, and incident reporting, fostering a security-first mindset.
- **Data Security (PR.DS):** Implement measures like encryption, data loss prevention (DLP), and secure lifecycle management to protect sensitive airport data (e.g., SSI, PII, financial, operational data).
- **Protective Technology (PR.PT):** Strategically deploy, configure, and maintain security solutions like firewalls, endpoint detection and response (EDR), and network segmentation for both airport IT and critical OT environments.

NIST CSF: DETECT Function: Identifying Cybersecurity Events at Airports

- **Anomalies & Events (DE.AE):** Establish operational baselines for critical airport IT and OT systems (e.g., network traffic, system performance) to effectively identify deviations indicative of potential security events.
- **Continuous Monitoring (DE.CM):** Implement and manage Security Information and Event Management (SIEM) systems and Intrusion Detection/Prevention Systems (IDS/IPS) for active surveillance of airport networks and key assets.
- **Detection Processes (DE.DP):** Define clear procedures for triaging security alerts, performing initial analysis to determine credibility and potential impact, and escalating confirmed incidents rapidly to the response team.

NIST CSF: RECOVER Function: Restoring Airport Operations & Resilience

- **Recovery Planning (RC.PL):** Ensure cyber recovery procedures are integrated into the airport's comprehensive Business Continuity and Disaster Recovery (BCDR) plans, prioritizing restoration of critical airport services.
- **Execution:** Methodically implement and test procedures for restoring affected airport systems and data from secure, verified backups, focusing on critical operational functions first (e.g., FIDS, gate assignments, security systems).
- **Improvements (RC.IM):** Continuously update and refine recovery plans and capabilities based on lessons learned from actual incidents, exercises, and any changes in the airport's IT/OT environment.
- **Communications (RC.CO):** Maintain clear and timely communication with all stakeholders (staff, leadership, tenants, passengers, regulatory agencies) regarding service restoration progress and any ongoing operational impacts.

NIST CSF: RESPOND Function: Taking Action During Airport Incidents

- **Response Planning (RS.PL):** Activate and execute the airport's pre-defined and regularly tested Cyber Incident Response Plan (CIRP) upon confirming an incident.
- **Communications (RS.CO):** Implement established communication protocols to inform internal teams (IT, Ops, Legal, PIO), airport leadership, and external entities (TSA, FAA, FBI, affected partners) as appropriate.
- **Analysis (RS.AN):** Conduct thorough forensic analysis during and after the incident to determine the attack vector, scope of compromise, data impacted, and extent of unauthorized access.
- **Mitigation (RS.MI):** Take immediate action to contain the incident (e.g., isolating affected systems, blocking malicious traffic) and eradicate the threat from the airport environment.
- **Improvements (RS.IM):** Perform a post-incident review to identify lessons learned and implement improvements to security controls, policies, and response procedures.

Conclusion

- **Recap:** Implementing airport cybersecurity involves a proactive approach to Governance, detailed Risk Management, strict Compliance adherence, and systematic Framework application.
- **Key Implementation Steps:**
  - Align leadership and develop enforceable policies.
  - Rigorously assess and manage risks to administrative and operational systems.
  - Operationalize TSA directives and protect sensitive information like SSI.
  - Utilize frameworks like NIST CSF to structure and mature your cybersecurity program.

Module 6 Preview & Questions

- We will shift to managing more advanced airport cybersecurity operations at airports and preparing for the future
- Check LMS for readings, supplemental resources, discussion board, and quiz.
- Questions?