PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0010 October 2017

Guidance for Protecting Access to Vital Systems Impacting Airport Security

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Faith Group, LLC
St. Louis, MO

COPYRIGHT INFORMATION

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about airport security technologies and procedures.

Through the Airport Security Systems Integrated Support Testing (ASSIST) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying perimeter and access control security technologies and procedures.

Through the Program for Applied Research in Airport Security (PARAS), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee, but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request for proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies Special Programs Manager*

PARAS 0010 PROJECT PANEL

Frank Capello *Broward County Aviation Department*
Justin Robert Chimka *University of Arkansas*
Kim Dickie *John F. Kennedy International Airport*
Renè Rieder, Jr. *Arup*
Christian Samlaska *Seattle-Tacoma International Airport*
Peter Troyer *Spokane International Airport*

AUTHOR ACKNOWLEDGMENTS

Thank you to the following airports for their willingness to participate in an in-depth survey:

- Charlotte Douglas International
- Philadelphia International
- Miami International
- Asheville Regional
- Savannah Hilton Head International
- Nashville International
- Oakland International
- General Mitchell International
- Minneapolis–St. Paul International

CONTENTS

LIST OF TABLES & FIGURES

PREFACE

Airports host systems—such as access control, video surveillance, and telecommunications—that are vital to airport security and critical to daily operations. While evidence of these systems can be seen as controlled doors and camera enclosures throughout the airport, the systems' foundations are tucked away in telecommunications rooms, data centers, weatherproof enclosures in an outside-plant location, or even off the airport property. The administration of proper access to systems for authorized users should be managed from both physical and logical perspectives.

Ironically, while these systems provide security to the entire airport environment, measures to protect them are often overlooked, which could result in critical failure. This guidebook addresses this underlying problem.

For example, a fully fault-tolerant server with redundant power supplies and backup is still vulnerable if its physical location is not properly controlled or unauthorized individuals gain access. Therefore, when protecting systems that are vital to airport security, airport owners and operators should be equipped with the most up-to-date knowledge, including applicable standards, operational best practices, and technology solutions to protect those vital systems.

This guidebook attempts to address the issues affecting vital security systems and empower airport operators with information, guidelines, standards, toolkits, and templates to overcome this threat.

HOW TO USE THE GUIDEBOOK

The icons shown in Table 1 are used throughout the document to direct attention to specific guidance areas.

Table 1. Airport Guidance Area Icons

Airport Specific	Physical Security	Electrical Security
✈	▥	⚡
Cyber & Network Security	**Policy/Best Practices/Standards**	**Staffing/Human Resources**
🔒	📂	👥

Additional icons (Table 2) are featured to help quickly identify specific areas of interest.

Table 2. Guideline Icons

⚠	**Problem Area** – Signifies an area where a problem may arise within the process of protecting access to vital systems or a potential roadblock
💡	**Good Idea** – Signifies an idea from lessons learned, a best practice or an industry standard
🎯	**Key Imperative** – Signifies a subject or area of knowledge that would be crucial or important to the airport operator as they move forward with applying governance, risk management and/or compliance

PARAS ACRONYMS & ABBREVIATIONS

The following acronyms and abbreviations are used without definitions in PARAS publications:

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
ANSI	American National Standards Institute
AOA	Air Operations Area
ARFF	Aircraft Rescue and Fire Fighting
CCTV	Closed Circuit Television
CDC	Centers for Disease Control and Prevention
CD/DVD	Compact Disc/Digital Video Disc
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
ID	Identification
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
R&D	Research and Development
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
SSN	Social Security Number
TCP/IP	Transmission Control Protocol/Internet Protocol
TSA	Transportation Security Administration
XML	Extensible Markup Language

GUIDEBOOK PURPOSE AND ORGANIZATION

Guidebook Purpose

This guidebook provides airport operators with a framework for understanding the systems vital to airport security and how to apply a risk strategy to each one using security controls. The guidebook also covers successful practices and lessons learned from surveyed airports.

While all airport technology is important, applications and systems related specifically to airport security and safety will always come to the forefront when identifying mission-critical, essential systems. This guidebook focuses specifically on the means of protecting access to those airport security applications, supporting systems, and infrastructure that are directly responsible for ensuring public and passenger safety and security. This guidebook also offers helpful ideas, templates, toolkits, and standards to empower airports to protect their vital systems.

Over the years, the systems responsible for directly securing airports have been slowly integrating with other airport systems since their various components have increasingly become reliant on an airport's local area network (LAN) and, in many cases, on the internet.

To protect the airport from threat events and to reassure the traveling public, airports must have a "Baseline Airport Security Plan" that is carefully choreographed for everything from system design, operation, integration, and collaboration with other non-airport operations entities such as airlines, service tenants, the TSA, and external emergency responders.

To establish a baseline plan mentioned above, it is important to define *Airport Security* for the context of this guidebook. The physical technology and logical elements that go into creating a security system can be complex to plan, design, implement, and maintain. For this reason, this guidebook assists those responsible for protecting access to these systems with a definition of airport security that covers the 1) Administrative (e.g., policies and standards), 2) Technological (e.g., data and network), and 3) Physical (e.g., gates, locks, fences) controls needed to maintain adequate day-to-day management and administrative operations.

This guidebook also covers the practices for administering and managing various types of access to vital systems such as video surveillance, access control, ID badging and credentialing, and the physical spaces where these systems reside. Also included are identifying, assessing, and prioritizing methodologies, and creating a governance framework that encompasses all risk management and compliance areas, so that systems are properly identified and adequate care is applied consistently.

These practices include both physical controls for protecting systems, as well as logical controls to protect against individuals accessing systems for which they are not authorized. Logical controls safeguard the data and the systems, networks, and environments that protect the airport. In order to authenticate, authorize, or maintain accountability, a variety of methods are used, such as password protocols, devices coupled with protocols and software, encryption, firewalls, or other systems that can detect intruders and maintain security, reduce vulnerabilities, and protect the data and systems from threats.

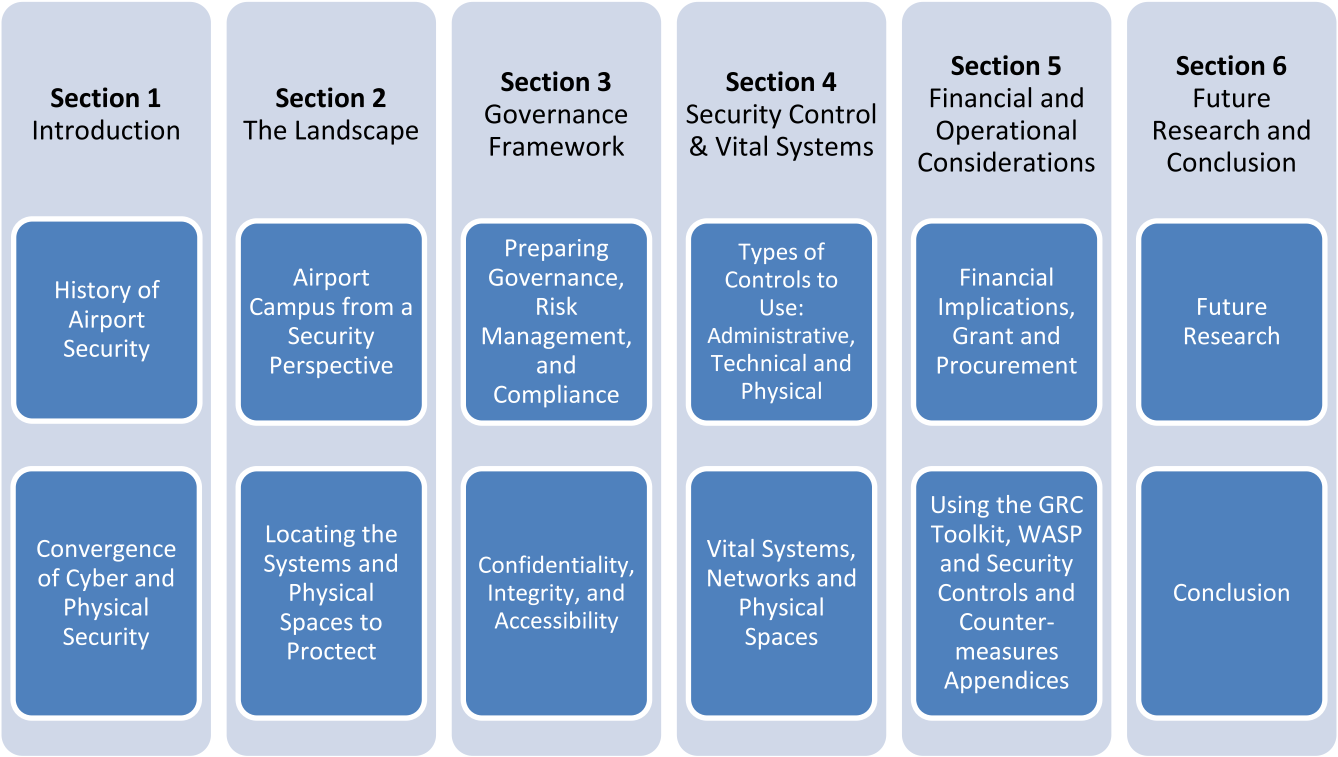
One of the challenges when applying both types of controls (physical and logical/cyber) is that Cybersecurity is typically applied by the airport technology department, whereas Physical Security may be administered by either public safety or the facilities organization. As a result, the security of security systems is split between two or even three airport organizations, potentially resulting in "gaps in responsibility."

Examples of industry standards and best practices used successfully at small, medium, and large hub airports across the country are included throughout this guidebook to address topics such as physical and logical access control, maintainability, and operational effectiveness.

Guidebook Organization

This guidebook is divided into six main topic sections, as shown in Figure 1, with appendices.

Figure 1. Guidebook Organization Roadmap



Section 1 Introduction	**Section 2** The Landscape	**Section 3** Governance Framework	**Section 4** Security Control & Vital Systems	**Section 5** Financial and Operational Considerations	**Section 6** Future Research and Conclusion
History of Airport Security	Airport Campus from a Security Perspective	Preparing Governance, Risk Management, and Compliance	Types of Controls to Use: Administrative, Technical and Physical	Financial Implications, Grant and Procurement	Future Research
Convergence of Cyber and Physical Security	Locating the Systems and Physical Spaces to Proctect	Confidentiality, Integrity, and Accessibility	Vital Systems, Networks and Physical Spaces	Using the GRC Toolkit, WASP and Security Controls and Counter-measures Appendices	Conclusion

Table 3 summarizes each section and offers a recommended audience with bullet points highlighting the topics presented.

Table 3. Guidebook Content Summary

Section Title and Description	Topic and Audience
Guidebook Purpose and Organization This section provides the overall objective of this guidebook and purpose of the guidance recommended. It gives the readers a quick summary of each Guideline section. This section also identifies the Airport Guidance Areas (classifications) and roadmap for the reader.	**Topics:** Guidebook organization **Audience:** Everyone

Section Title and Description	Topic and Audience
Section 1: Introduction and History of Airport Security This section provides a historical perspective and evolution of aviation security. It illustrates historical incidents involving airport security and relevant federal laws, regulations, and organizations that evolved in reaction to these incidents. The section goes on to introduce the significant investments in security by airports and the threats and vulnerabilities associated with such investments (typically not covered by an Airport Security Program).	**Topics:** Aviation security history Historical security incidents Relevant laws and regulations **Audience:** Executive management and/or new to airport security
Section 2: The Landscape (Environment) This section covers areas of the airport where security systems and spaces are located. This section further defines the security systems, their role in airport security, and their location. It also identifies relevant supporting systems upon which the applications exist, the computing infrastructure (servers and storage), and all the supporting software (operating systems, middleware, and utilities), including Network Access Control (NAC) methods.	**Topics:** Airport security areas Systems and spaces containing security elements Systems vital to airport security Threat types Threat vectors Threat countermeasures **Audience:** Executive management and/or new to airport security
Section 3: Governance Framework This section covers the Governance, Risk Management, and Compliance (GRC) areas for setting up a framework to effectively manage the risks and threats associated with system and physical spaces.	**Topics:** Airport campus Systems and spaces containing security elements **Audience:** Executive management and/or new to airport security
Section 4: Security Controls and Vital Systems This section provides an introduction to security controls, explains how to develop them through administrative, technical, and physical groupings, and provides examples. Additionally, a listing and definition of vital systems and networks (including the physical spaces where they reside) is included to provide context for the administration of controls.	**Topics:** Security controls introduction How to use security controls How to define security controls that are administrative, technical and/or physical in nature **Audience:** IT and security management Security and compliance Information technology Public safety

Section Title and Description	Topic and Audience
Section 5: Financial and Operational Considerations This section provides ways an airport provider can put governance, risk management, and compliance practices into action, providing examples of each, from planning the funding and procurement vehicle, through testing and quality assurance of implementation, to maintaining an operational life cycle. This section includes references to tools in the appendices needed by the airport operator to put GRC into action in reference to protecting access to systems and physical spaces.	**Topics:** GRC in action Concept of operations Asset management Threat and vulnerability assessment Countermeasures Best practices **Audience:** IT and security management Security and compliance Information technology Public safety
Section 6: Future Research and Conclusion This section takes a brief look at future ways an airport can protect access to vital systems and spaces, including using unmanned vehicles, sonar and radar, and resilient and intelligent networks.	**Topics:** Future research considerations **Audience:** Airport operators and staff
Appendix A: Governance, Risk Management, and Compliance (GRC) Toolkit This appendix offers a toolkit designed to help an airport operator start a formal governance workflow. This includes an example governance charter, organizational chart, committee, and roles and responsibilities, along with managing risk through asset and inventory management, concept of operations, threat and vulnerability assessments, and maintaining GRC through compliance and a Written Information Security Program (WISP, Appendix C).	**Topics:** Developing a governance model Understanding and applying risk management and compliance **Audience:** Executive management Security and compliance Management IT management
Appendix B: Security Controls & Countermeasures Matrix This appendix provides a matrix document to help airport security and information technology professionals identify threats to vital airport systems and physical areas impacting airport security, assigning security controls, and developing mitigation/countermeasures.	**Topics:** Security controls through directive, deterrent, preventative, compensating, detective, corrective, and recovery techniques Adherence to security controls that are administrative, technical and/or physical in nature **Audience:** Security and compliance IT security Public safety

Section Title and Description	Topic and Audience
Appendix C: Written Information Security Program This appendix provides a document template and guidance on creating a WISP. Utilizing the NIST framework for protecting Information-Based Security Management Systems (ISMS), this template includes: • Protecting the confidentiality, integrity, and availability of the airport's data and systems • Protecting the airport, its employees, and its clients from illicit use of airport systems and data • Ensuring the effectiveness of security controls over data and systems that support the airport's operations • Recognizing the highly networked nature of the current computing environment and providing effective airport-wide management and oversight of those related information security risks • Providing for the development, review, and maintenance of minimum security controls required to protect the airport's data and systems	**Topics:** Developing a written plan for security Ensuring effectiveness of security controls Adhering to national standards **Audience:** Security and compliance Information technology security Public safety

SECTION 1: INTRODUCTION AND HISTORY OF AIRPORT SECURITY

1.1 Introduction

For decades, airport operators have utilized increasingly more complex methods of securing the airport campus, with the earliest airfields being a relatively open range as compared to today's highly restricted footprint. Although, historically, the focus of the airport security system has been to protect aircraft, airports now provide shelter, services, and various levels of security to passengers, visitors, airport and airline personnel, physical facilities, equipment, and merchandise.

In addition to the airport itself, the operator is also protecting the economic investment of the local community and safeguarding the emotional feeling of safety for the traveling public. Particularly since the attacks of September 11, 2001, more sophisticated methods of controlling access have been mandated through federal regulation, with some airports applying far-reaching measures that are also driven by internal policy.

When a security event occurs at an airport involving a potential or perceived threat to life-safety, the utmost attention is given to resolving the issue as quickly as possible. Oftentimes, the post-incident review focuses primarily, or even entirely, on how the human resources (first responders, incident command, and airport personnel) responded to the event. Procedures and processes are often revised to respond to any perceived weakness in the response approach. Also, physical attributes of the airport space, including fences, bollards, checkpoints, lighting, entryways and exits, and a host of other physical features are carefully reviewed. While technology-based security systems also may receive some scrutiny, the review is typically focused on the responsiveness and performance of the system and not on the security of the system itself.

Traditionally, airport operators have invested significant resources into designing and maintaining security systems, such as Physical Access Control Systems (PACS), Identity Management and Credentialing Systems (IDM-CIS), CCTV, Video Surveillance Systems, and others.

⚠ *Ironically, while these systems are at the very foundation of security for the entire airport, providing security for these systems themselves is often overlooked, which could result in critical failure. This is the underlying problem that this guidance intends to address.*

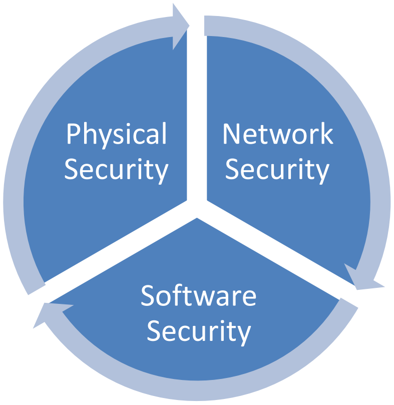
The supporting product literature and expertise in deploying such systems is publicly available, hence these systems are easily compromised. As an example, third-party software that impacts airport security systems and the servers where they reside includes common applications such as Adobe Flash, Microsoft Silverlight, Adobe Reader, and Java. Per Microsoft's 2016 Trends in Cybersecurity, third-party software is often the source of cybersecurity vulnerabilities and requires significant attention in terms of patching and retesting airport applications.

Airport operators must keep pace with protecting their investments in technology against nefarious activity, vulnerabilities, and threats.

1.2 Physical, Network, and Software Security Convergence

Within the last decade, the physical, network, and software security worlds have converged, presenting airport operators with an integrated solution for securing the airport environment, providing instant alerting of potential threats, and offering greater situational awareness.

This technological evolution, however, has significantly added to the complexity of daily management and administration of multiple systems working together.



As telecommunications and data networks have expanded and evolved to provide business access to the internet, internal network file sharing, and email, so too have airport security systems joined the same networks to take advantage of the speed of information during situational analysis, remote access, and communication with physically separate devices. Thus, the underlying network environment has become an integral component of the security system.

Given the advancements in converged and integrated networks (e.g., Secure Virtual Local Area Networks, Software-Defined Networks, Software as a Service, Platform as a Service, etc.), airport operators are seeking to develop formalized plans for disaster recovery and business continuity that cover their vital systems as well as hardware, software, network technologies, and access control areas.

For example, in a 2016 failure, a potentially outdated power control module in an airline's data center failed, causing a small fire that was quickly extinguished. The airline had a backup power system in place, but approximately 300 out of 7,000 of their servers weren't wired to backup power. This flaw in the company's planning caused the entire computer system to a grind to a halt. (Paraphrased from MyAJC, 2017)

1.3 Nefarious Activity Involving Physical Spaces and Security Systems

Over the last few years, there has been a rise in incidents involving secure airport areas, from cyberattacks to physical attacks with vehicles. "Nefarious activity" implies a criminal element is involved and has been a catalyst for protecting the ever-changing landscape of security at an airport since September 11, 2001. Recent examples of such attacks are summarized here, and include airports (US and International), as well as other critical infrastructure areas in the United States.

Cyber Attack

The websites of two airports in Asia Pacific were targeted via a denial-of-service attack in response to the detention of an American anti-whaling and dolphin activist, thereby rendering the websites unavailable for passengers and airlines (Carolina, 2015).

Power Grid Attack

A cyberattack causing a voltage spike, which in turn damaged connected consumer appliances and electronics, resulting in major cost implications (i.e., physical asset damage, remediation, third-party liabilities, and business interruption). Refrigerators, computers, TVs, and other appliances are easily damaged when such events occur.

Physical Security Breach

Video footage shows a woman in the cell phone lot tossing a plastic bag over a secured fence to an airline worker. Unlike the arrivals and departures area of the airport, which are blanketed with security directing traffic, screening passengers and patrolling the grounds, the new cell phone lot sits largely unattended.

Physical Fence Breach

A 15-year old climbed a fence, hoisted himself into a jet's wheel well and survived an almost six-hour flight to Hawaii.

Insider Threat / Badging and Credentialing

Airport workers, government officials, and top airport officials abused their security badge privileges and allowed family and friends to bypass TSA security checkpoints. One airline employee was fired over using his badge to allow his entire family into a van on the airport ramp to drive to the terminal to catch a flight.

Physical Breach and Unauthorized Plane Entry

A man on the run after stabbing a plumber scrambled over a barbed-wire fence and dashed onto an empty plane.

Domestic Terrorism

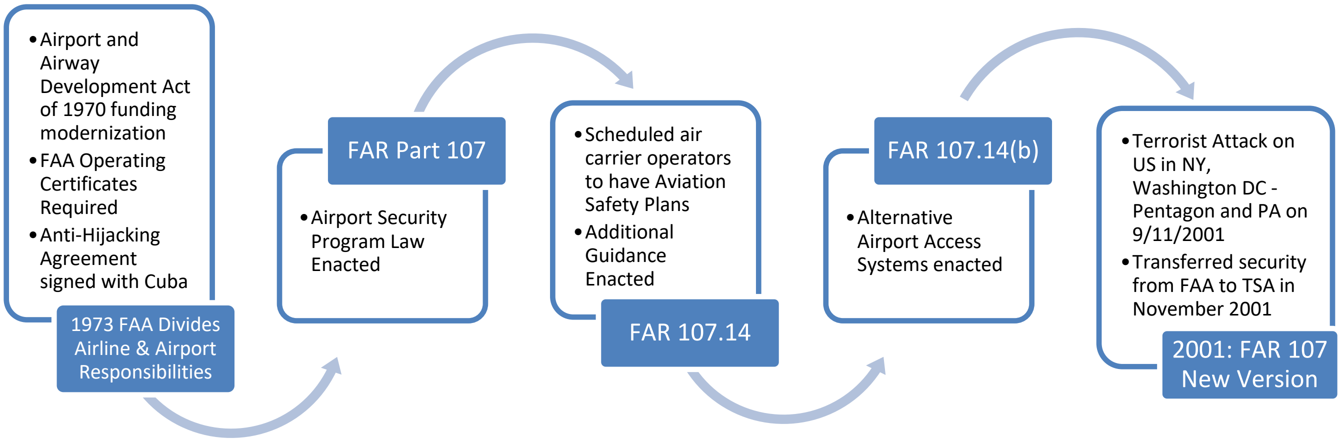
An airport avionics technician was arrested after 5 months of conspiring to use his access credentials to drive a vehicle onto the ramp and place explosives in a plane. He portrayed himself as "the access guy" and expressed a desire to "engage in violent jihad on behalf of al Qaeda." He eventually decided the best plan to "maximize casualties" would be to detonate a vehicle between the airport's two terminals during the early morning peak passenger hours.

While nefarious activities often present newsworthy stories in the media, other threats are also present for security systems. These include natural and man-made disasters, failed hardware and software, personnel errors, poorly operating applications, and a host of other threats. This guidebook describes security mechanisms that address these threats through the Confidentiality, Integrity, and Availability (CIA Triad) of security systems, which is the goal when establishing an airport security program.

1.4 A Brief History of Airport Security Regulations

Historically, airport security has primarily focused on preventing unauthorized access to the secure areas of the airport. The late 1960's and early 1970's saw a rise in hijacking of commercial aircraft because physical access control to the airport operational areas was minimal. At that time, no passenger identification was required, scanning with an electronic magnetometer was used only if traveler actions looked suspicious (these devices were not routinely available), and body pat-downs were employed most often. While security became an issue of paramount importance after the events of September 11, 2001, inclusion of x-ray machines and metal detectors and universal passenger screening were mandated in 1973. Additionally, airport owners and operators were required to have an FAA-approved Airport Security Program (ASP), with Federal Aviation Regulation (FAR) Part 107 referencing a more secure environment in which airlines should operate. Figure 2 shows the evolution of airport security regulations through 2001.

Figure 2. Timeline of Airport Security Regulations: 1970–2001


• Airport and Airway Development Act of 1970 funding modernization
• FAA Operating Certificates Required
• Anti-Hijacking Agreement signed with Cuba
1973 FAA Divides Airline & Airport Responsibilities
FAR Part 107
• Airport Security Program Law Enacted
• Scheduled air carrier operators to have Aviation Safety Plans
• Additional Guidance Enacted
FAR 107.14
FAR 107.14(b)
• Alternative Airport Access Systems enacted
• Terrorist Attack on US in NY, Washington DC - Pentagon and PA on 9/11/2001
• Transferred security from FAA to TSA in November 2001
2001: FAR 107 New Version

In 2001, the Aviation Transportation Security Act (ATSA) transferred security responsibility from the FAA to the DHS TSA.

In reference to CFR 49 §§ 1500–1599, specifically § 1542.207, the division of responsibility now included federal agencies (e.g., TSA) as well as airlines and airports. Although references to PACS design in these documents remain largely unchanged, the implementation details have been the focus of TSA Security Directives over the years (see Figure 3, page 13).

Since February 2016, various working groups in collaboration with DHS/TSA have taken steps to address the potential threat posed by airport employees, contractors, and vendors with airport access privileges. This is termed "Insider Threat."

Additionally, international and US-based standards organizations, including NIST, ISO, International Electrotechnical Commission (IEC), International Civil Aviation Organization, and Federal Information Processing Standards (FIPS) 201 and 201-2, have influenced how airport security is designed, implemented, and used at airports. However, the focus of these regulations has been solely on protecting the physical space that these systems are guarding, and offer very little to recommend how the systems themselves should be protected.

SECTION 2: THE LANDSCAPE (ENVIRONMENT)

2.1 Introduction

For many involved with security in the air transport industry, the landscape of an airport is mostly analyzed from a physical perspective. Fences, barriers, security checkpoints, police, and TSA are seen every day by the traveling public.

The underlying systems used in airport security are given far less consideration. Many assume that the security measures to protect access to secured areas, locks/keys, access controlled card readers, and video surveillance, are also sufficient to protect the systems without additional safeguards. However, because of the convergence of security systems with the airport's IP-addressable network, there are far more security issues that must be addressed to ensure airport security.

This guidebook section covers not only the physical landscape where these systems reside, but also the systems themselves and all the components a system uses to effectively run the airport 24/7/365. Comingling these systems with the governance framework for aviation safety and security, and ensuring compliance with relevant security regulations, standards, and guidelines all interrelate to create and enable a comprehensive airport system's security footprint. Whether airports are large Cat X or small General Aviation operations, the principles defined in this research apply but can be tempered based on the complexity of their respective operations. Recommended actions can be followed easily by airport operators of any size using the GRC tool kit found in Appendix A.

2.2 Regulations, Guidelines, and Standards Brief

Airport staff from different disciplines typically follow basic guidelines to improve protection of security systems, including the DHS/TSA Airport Security Design Guidelines (2011) and the National Safe Skies Alliance guidebook *Recommended Security Guidelines for Airport Planning, Design, and Construction* (2017) for airport operations and security staff, and the NIST Cybersecurity Framework or ISO 27001-02 IT Security Guidelines for airport IT staff. Other guidance is found in reports and studies produced by the federal government, such as the Government Accountability Office (GAO) document entitled "Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates."

While these guidelines and standards are useful, an airport operator should also follow the governance framework outlined in the next section to align them with current or future airport goals and initiatives. This process can improve the overall security footprint at an airport and protect the systems that support airport security.

2.3 Risk Assessment (Threat/Vulnerability Assessment)

Executing a successful governance framework, which includes protecting the various assets found on the airport, includes a thoughtful risk assessment process such as a Threat/Vulnerability Assessment (TVA). By using all available stakeholder intelligence resources for local and national threats, and scheduling periodic refresh cycles to keep the airport security viable, a thorough and useful TVA can be completed.

*While a TVA will provide the vehicle for documenting assets, physical locations, and give a level of risk associated with a system, it is important to first define 1) airport security areas, and 2) the vital systems that are impacting airport security***.**

With a good understanding of these two key areas, an airport operator can create the baseline from which to start the governance process in protecting access to these systems and their locations on the airport campus.

2.4 Airport Security Areas

There are many critical assets and operationally sensitive security areas that airport operators are responsible for protecting. As a public facility, a balance between effectively mitigating risk and allowing for public access is a constant challenge. It is a reality that the human risk (that of passengers, public, and staff as insider threats) must be continually assessed and managed in a manner that provides public access to a transportation facility while protecting its operational integrity from covert or overt attack. It is this balance that routinely challenges the airport operator, transportation manager, security system architects, and facility operators. The FAA has defined airport security areas as shown Table 4.

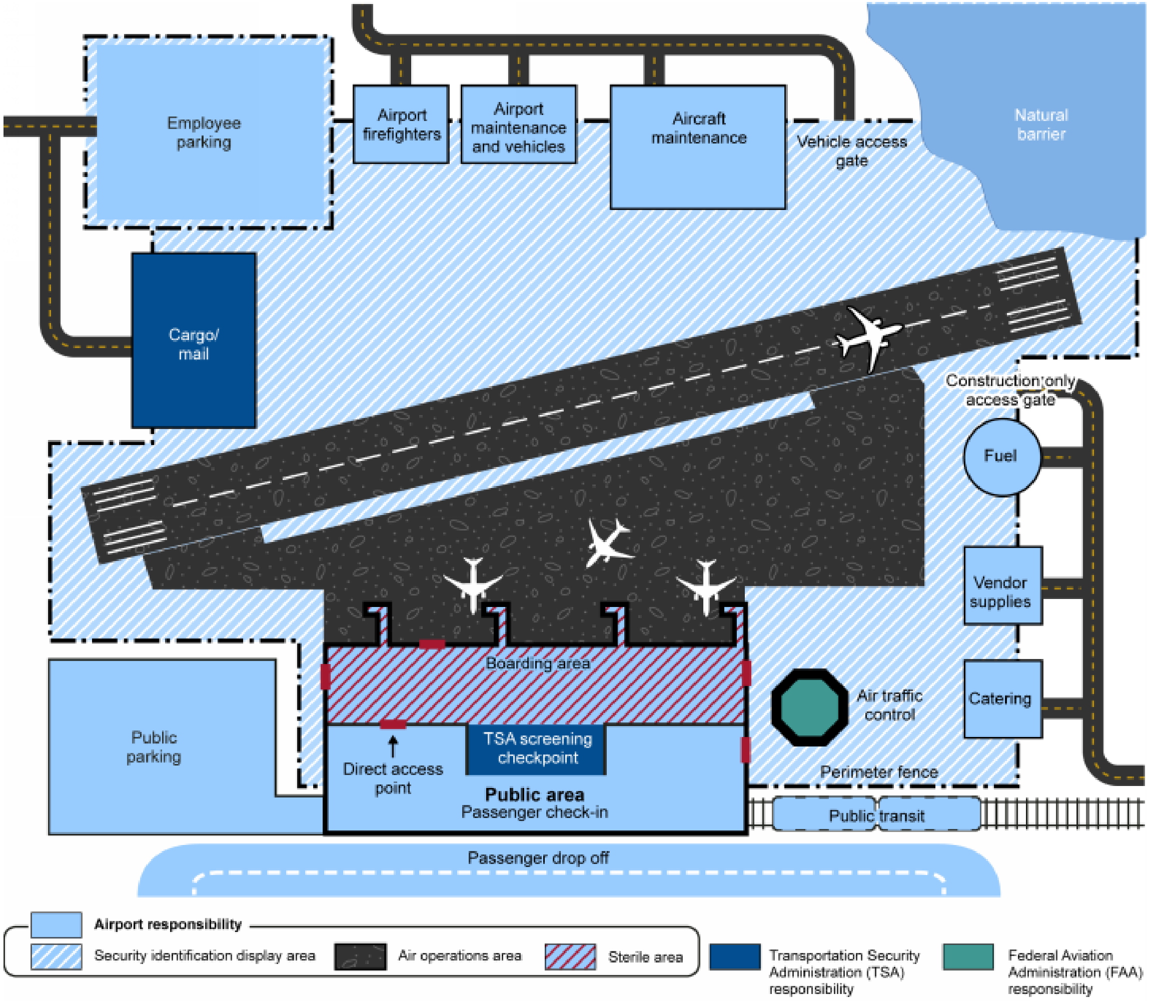
Table 4. Airport Security Areas Matrix

	Airport Areas	Landside	Airside (AOA/SIDA)	Concourse (Sterile Area)	Roadways
Perimeter	Perimeter Fence	X	X		
	Internal Fence		X		
	Vehicle & Pedestrian Gates	X	X		
	Outside Security Enclosure	X			X
Terminal/SIDA Facilities	Employee Access Portals (Mantraps, Turnstiles)		X	X	
	Concourses		X	X	
	Terminal Roadways				
	Internal Roadways		X		
	Curbside	X			
	Terminal Lobbies	X			
	Security Operations Center	X	X	X	
	Airport Operations Center	X		X	
	Baggage Claim Areas	X	X		
	Security Checkpoints			X	
	International Arrivals Area		X		
	Telecommunications Rooms / Data Centers	X	X	X	

	Airport Areas	Landside	Airside (AOA/SIDA)	Concourse (Sterile Area)	Roadways
AOA/ Outside SIDA	Outside Plant	X	X		X
	Passive Network (Utility/Telecommunication Paths)	X	X	X	X
	FAA NAVAIDS		X		X
	FAA Control Tower Sites	X			X
	Fuel Storage Facility	X	X		X
	Mail & Cargo Areas	X	X		X
	Air Carrier Aircraft Parking Areas		X		
	Aircraft Rescue & Fire Fighting	X	X		
	Intermodal Transportation Facilities		X		X
Physical / Logical	Servers	X	X	X	
	Workstations	X	X	X	
	Switches/Routers	X	X	X	
	Mobile Devices	X	X	X	X
	Uninterruptable Power Supply	X	X	X	
	ID Badging/Credentialing	X	X		
	Active Network	X	X	X	

From the perspective of a large airport campus, Figure 3 depicts the security-restricted areas of a typical commercial airport in the United States and the areas of an airport where aviation security should be focused; thus, providing a high-level view of the security.

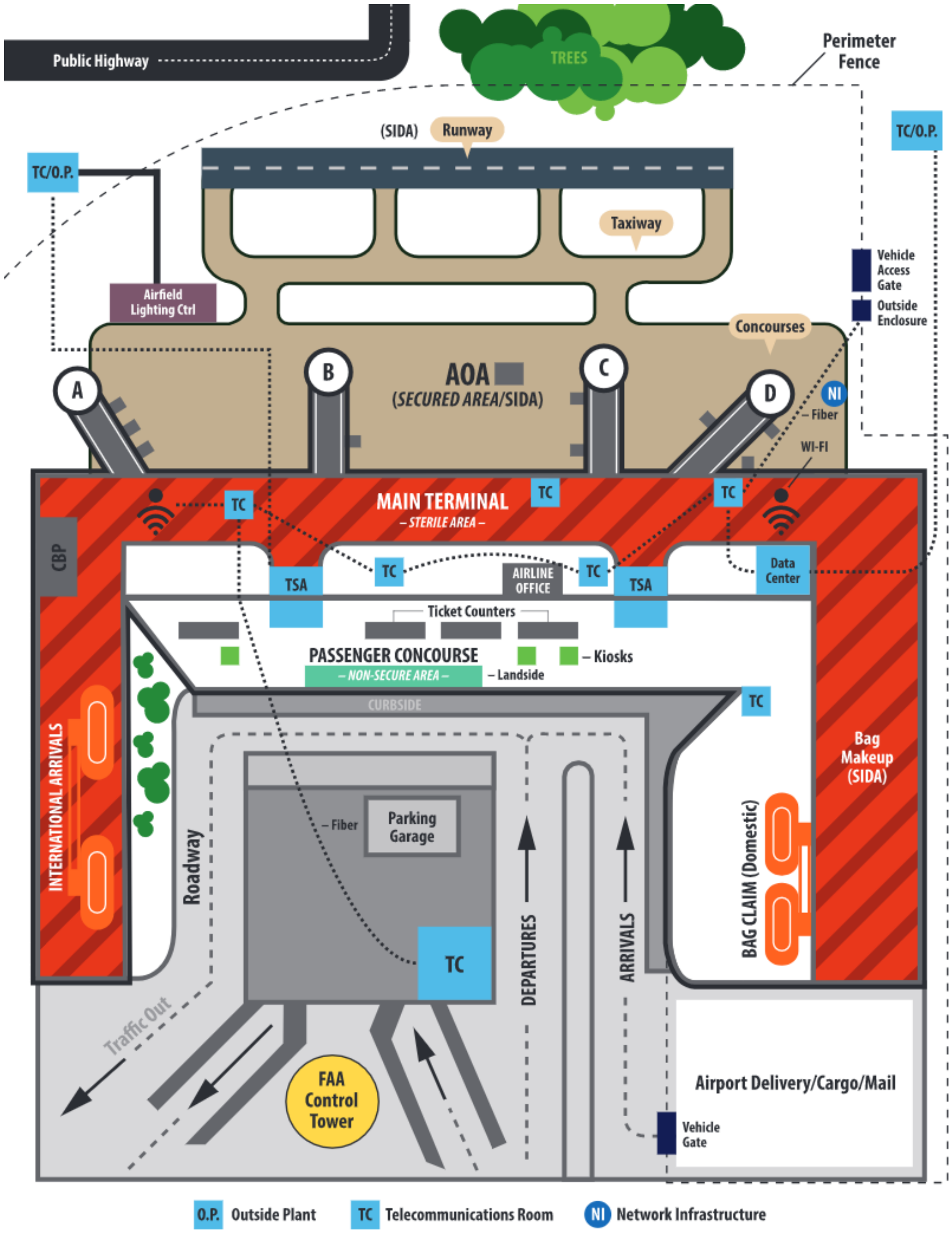
Figure 3. Security-Restricted Areas of a Commercial Airport in the United States



While perimeter security tends to focus on the SIDA, AOA, and Sterile areas of the airport, airport operators must not ignore potentially critical assets located on the non-sterile public or landside of the airport operations.

If these sites are commonly known, well-marked, or otherwise advertised to the casual observer, they too can become a vulnerability (e.g., airport utility plant, etc.) An additional map shown in Figure 4 gives more transparency to areas where security-related systems may reside or are used.

Figure 4. Example Locations of Vital Systems



For example:

- Outside Plant
- Telecommunications Room
- Data Center
- Vehicle Access Gate
- Outside Enclosure
- Wireless Access Point
- Fiber and Conduit Pathways

Managing physical access to secured or “airport operator only” areas has largely been an airport operations, security, or law enforcement concern, accomplished through a mix of daily inspections, checklists, and system tests (e.g., Crash Phone test with the Air Traffic Control Tower). In most cases, the viability and operational integrity of both the security systems and the underlying telecommunications and data networks connecting them has been delegated solely to the IT department or outsourced to a third party.

2.5 Systems Vital to Airport Security

All the physical locations described above must be secured, either by physical security, logical security, or a combination of the two (including human resources such as airport staff). However, the delineation between physical and logical/technical security, in reference to computerized software applications used for security, has narrowed over time. Standalone software and systems designed to provide certain types of security (e.g., Access Control Systems for ingress/egress through doors and gates), have been joined with other software applications (e.g., ID/Credentialing) through the network backbone and integrations to form "Systems," such as the PACS or the Security Information and Event Management (SIEM) system.

Table 5 gives a brief overview of the components that make up the systems that impact airport security. Definitions and security controls of these systems are covered in Section 4: Security Controls and Vital Systems.

Table 5. Components of Vital Airport Systems

	Physical Locations	Physical Components	Logical/Technical Components
Premises Distribution (Wiring & Backbone) Systems (Passive Network)	Airport Campus Wide Telecommunication Rooms Data Centers Central Office/Outside Plant	Fiber/Ethernet Wireless Backhaul Conduit/Pathways	Switches/Routers Telco Demarcation
Local Area Network (Active Network)	Airport Campus Wide Telecommunication Rooms Data Centers Central Office/Outside Plant	Switches/Routers Firewalls Storage Area Networks (SAN) Network Attached Storage (NAS) Remote Access Appliances Servers/Workstations/ Mobile	
Physical Access Control Systems (PACS)	Airport Campus Wide	Controllers Card Readers Request-to-Exit Devices Electromechanical Mortise Locks Magnetic Locks Electric Strikes Active/Passive Network Cyber Locks ID Badges	Firewalls Switches/Routers Access Control System (ACS) ACS Database ID/Credentialing & Badging Software
Video Surveillance Systems	Airport Campus Wide	Active/Passive Network Analog Video Cameras Specialty Cameras (Pan-Tilt-Zoom, Thermal)	Video Management System (VMS) IP Video Cameras VMS Database

Security Information and Event Management System (SIEMS)	Telecommunication Rooms Data Centers	Switches/Routers Workstations/Servers Firewalls	Log Files SIEM Database
Perimeter Intrusion Detection Systems (PIDS)	Airport Campus Wide Airport Perimeter	Active/Passive Network Fencing Gates Trenches Waterways	ACS Video Surveillance Systems SIEMS PIDS Database
Airport Communication Systems	Airport Campus Wide	Active / Passive Network Phones Radios Antenna Farms	PBX/VoIP Head End Radio Management Software
Emergency Response Systems	Airport Campus Wide Police/Fire/Rescue Stations Parking Garages Airport/Emergency Operations Centers	Emergency Phones Crash System Phones/Public Addressing Blue Light Phones/Kiosks	Active/Passive Network Mass Communication Software Computer Aided Dispatch Software GIS Software
Airport Operations Systems	Airport Campus Wide Airport/Emergency Operations Centers	Active/Passive Network Crash System Phones/Public Addressing	Active/Passive Network Airport Operations Software Crash Phone Software

Supporting systems include the underlying communication network (switches and routers, etc.) upon which the applications exist, the computing infrastructure (servers and storage), and all the supporting software (operating systems, middleware, and utilities), including NAC methods. Physical Infrastructure includes the underlying physical components such as Open Systems Interconnection (OSI) Layer 1 (copper and fiber), data centers, communication rooms, and the physical components needed to secure these facilities (locks and barriers).

One of the more critical aspects of the supporting systems is the logical access control mechanisms used to allow authorized users to gain access to security applications, confidential information, and network resources. Similarly, physical access to infrastructure elements must also be controlled through both physical and logical access mechanisms.

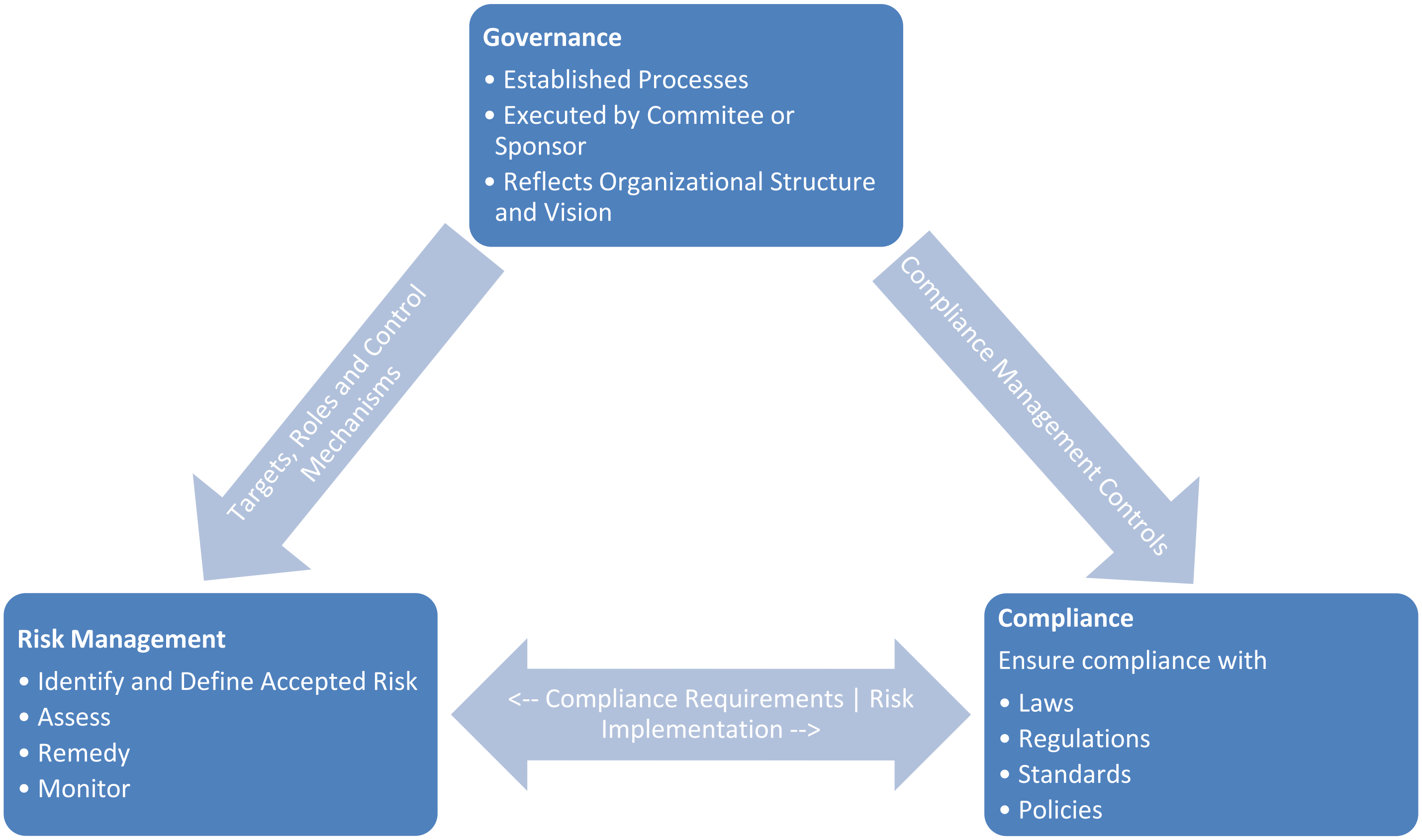
SECTION 3: GOVERNANCE FRAMEWORK

3.1 Introduction

Successfully protecting access to systems vital to airport security involves more than just a management and operations process to monitor and maintain systems. Providing a roadmap and toolkit to the people responsible for identifying, planning, operating, monitoring, and supporting these systems is essential. A starting point involves creating a governance framework that encompasses all risk management and compliance areas, so that systems are properly identified and adequate care is applied consistently.

This section is divided into three subsections: Governance, Risk Management, and Compliance. Each subsection describes the guidelines and steps needed to develop the framework. It is important to understand that inputs and outputs of each area tie directly in to the other areas; for example, the targets, roles, and control mechanisms outlined in Governance are direct inputs for Risk Management. Figure 5 shows how these areas are tied together:

Figure 5. Governance, Risk Management, and Compliance Diagram



Governance
• Established Processes
• Executed by Commitee or Sponsor
• Reflects Organizational Structure and Vision
Targets, Roles and Control Mechanisms
Compliance Management Controls
Risk Management
• Identify and Define Accepted Risk
• Assess
• Remedy
• Monitor
<-- Compliance Requirements | Risk Implementation -->
Compliance
Ensure compliance with
• Laws
• Regulations
• Standards
• Policies

Recently, vital airport systems have grown in complexity and usage. The number of stakeholders having a vested interest in general access control and monitoring has increased to include more than just airport police and operations staff. Access control addresses the restrictive measures used to ensure only authorized personnel can gain entry to these areas. However, the monitoring aspect of securing these areas presents an interesting challenge to facility operators—that of capturing, recording, and responding to notifications of a system breach.

Applying the “reasonable person” principle to access control can be difficult, as experienced by numerous airports when a breach occurs.[1] For example, when multiple fence line breaches occur at a Cat X airport by people with cognitive impairments, the facility operator does not have the luxury of feeling satisfied that a barrier is in place. Even though the individuals have no real intent to do harm, they are no less a threat to the public when they are on the AOA. Rather, the overall system must allow for effective monitoring of unauthorized access, attempts to circumvent security measures in place, and overt attempts to crash through physical security measures. This section will look at the growing standards and best practices put in place to protect access from a physical perspective.

3.2 Governance

Governance (or IT Governance) is an essential element in the management of an airport’s technology resources. Governance ensures that an organization has a clear vision of its technology priorities and goals; a full understanding of its technology and data assets; an understanding of the resources required to acquire new technology; how to properly maintain current technology; and how to ensure that its technology meets the CIA Triad: Confidentiality, Integrity, and Availability. For the purposes of this guidebook, it will be assumed than an airport does not presently have a governance organization.

While all technology functions are important to an airport, there is none more important than the physical security systems that protect the airport’s customers, personnel, visitors, tangible assets, and all the airline and concessionaire resources. Protecting these systems cannot be properly accomplished in a piecemeal or happenstance manner.

A well-developed plan must be established that accounts for the airport environment, the systems themselves, and the responsibility of airport organizations to carry out the plan. The plan must provide the necessary resources—both financial and staffing—to do the job. The plan is produced through the process of governance.

A small hub airport in the Southeast United States uses a combination of Operations, IT, and Airport Executives to establish directives for capital planning for security systems, including the security of those systems.

Governance need not be complicated, but some essential elements must be present to ensure that it functions properly. First, governance needs the support of the airport’s CEO. Without such support, governance has little chance of being successful, especially when difficult decisions must be made or resources are needed.

Second, governance should be carried out by a formally constituted board or committee of high-ranking airport managers. However, in the case of small airports or those with limited resources, representation from Airport Operations and IT, along with an external member (consultant or community leader) might be sufficient. Technology impacts virtually every aspect of airport operations; therefore, broad representation on a Governance Committee is desirable. Finally, the Governance Committee must meet on a regular basis and have the authority to make decisions that formulate technology direction and policy.

Many airports already have Governance Committees or something similar. Where such a committee exists, developing a plan for securing physical security systems may be an important subcomponent of

[1] *Reasonable Person* is a hypothetical person in society who exercises average care, skill, and judgment in conduct, and who serves as a comparative standard for determining liability.

the committee's overall function. Where no governance body exists, an airport should seriously consider establishing a committee specifically for this purpose.

As stated above, one of the most important factors is to have executive support. So, the first action in establishing a governance environment is to have the top airport official sanction the creation of such a body and assign one senior manager the role of establishing the parameters. Once the direction is given to move forward, the senior manager responsible must identify the management and resources that will comprise the governance body and ensure their working cooperation.

Typically, a Governance Committee will develop a written statement outlining its role and responsibilities, as well as its authority and the scope of its decision-making power. This can be included in a "charter" format that also includes committee by-laws regarding membership transition, meeting occurrence, the voting process, and other necessary rules and procedures that will assist in allowing the committee to act in the most effective manner. A Governance Charter Toolkit is provided in Appendix A.

Once the governing body is established, there are two essential tasks: Task 1) Developing an inventory of IT assets for physical technology security systems; and Task 2) Conducting a risk assessment of the entire physical security environment.

The first task requires a detailed description for each of the various systems (e.g., CCTV/Video Surveillance), which includes the following:

- An inventory of the hardware components, including model numbers, purchase dates, end-of-life estimates, initial cost, and any additional pertinent information that is essential for understanding the characteristics of the hardware
- An inventory of the software components, including license information, expiration dates, patching requirements, acquisition cost, and system owner
- A detailed listing of the information that is maintained on these systems, its sensitivity and/or confidentiality, data storage location, and retention and disposal policy
- An architectural depiction of the specific system and the level of integration with other physical security systems
- A complete description of the underlying infrastructure that supports the physical security systems, likely focusing on the network, its components, and its management structure
- A description of the airport staff and contractual resources that support each system, including cost, contract expiration, and contract requirements

Many organizations use an asset management application to track their asset's location and status. Many applications are available for free on the internet, as well as paid systems that may provide more benefits and features, such as integration with the airport's financial and/or fixed-asset system. Many airports use a Computerized Maintenance Management System (CMMS) or an IT-based Helpdesk system that can track both physical (e.g., switches, servers, and workstations) and logical (e.g., software licenses) components. Smaller airports may use a simple paper-based template Inventory/Asset Toolkit as provided in Appendix A, in addition to a list of software for CMMS and/or IT Helpdesk systems that are open source and available for free.

With this basic inventory in hand, Task 2 can begin, which is the risk assessment of the entire physical security environment. The risk assessment process uses a traditional approach that includes the following steps:

- Identifying airport assets (completed in the inventory discussed above)
- Identifying all threats that could impact the system's confidence, integrity, and—most importantly for physical security systems—availability (CRAMM Methodology in Appendix A)
- Identify the system vulnerabilities, looking at the CIA Triad
- Assigning a score to each of the threats that identifies the likelihood of their occurrence
- Assigning a score to each of the threats that identifies the impact
- Combining the likelihood and impact scores (there are numerous risk methodologies available for use; this guidebook will not offer a specific approach)
- Ranking the threats based on the likelihood and impact
- Developing a mitigation strategy for each of the threats that are deemed to be of importance
- Determining the cost for completing the mitigation actions and securing the necessary funding

Identifying threats is a critical step and must be approached in the broadest sense. Threats can be any of the following:

- Human (both internal and external)
  - Intentional system hacking or disruption
  - Unintentional system hacking or disruption
- Natural (disasters such as earthquakes and floods, etc.)
- Physical (fire and power outages)
- Technical (hardware or software failures and corrupted databases)
- Environmental (HVAC and flooding)
- Operational (unpatched resources, not properly backed up, lack of a disaster recovery plan and lack of a business continuity plan)

Vulnerabilities should be identified as related to people, processes, data, technology, and facilities. Each of these factors has a variety of vulnerabilities associated with it. For example, human resources that are not properly vetted with the necessary security clearances could pose a threat to available operations of a security system.

Likelihood can be a simple scale, such as Likely to Occur, Moderately Likely to Occur, Possible Occurrence, Rarely Likely to Occur, or No Possibility. Likelihood could also be determined using a time scale based on the potential for occurrence within a year, 1–3 years, 3–5 years, and greater than 5 years.

Impact can be identified using qualitative or quantitative methods. Typically, an airport will find that a qualitative approach is easiest, though it is subjective and is influenced by the opinions of those involved. A quantitative approach is more direct and easier to justify, but there are many aspects of risk that are not easily quantified. For example, if an airport were to have a major failure of its security systems at a critical time, it would be hard to quantitatively assess the reputational damage the airport would garner in the minds of its community and the traveling public.

With the risk assessment completed, the Governance Committee can now begin its work in securing physical security systems. The first step is for the committee to assign the responsibility to individuals and organizations within the airport to carry out the mitigation tasks. The necessary resources should be made available and a specific due date for completing the implementation can be established. It is essential that the Governance Committee seek accountability from those charged with carrying out the mitigation effort.

Note that the risk assessment is a snapshot in time and must be regularly updated, with new risks added, priorities changed, and new mitigation strategies developed. A new risk assessment may be conducted on a regular schedule, or especially when a new security technology is added to the environment. At a minimum, a risk assessment must be conducted annually.

The role of the Governance Committee does not end with identifying risk, obtaining resources, and assigning and overseeing responsibility. The committee will also direct the creation of the necessary policies and procedures that are an integral component in managing the IT and security environment. The Governance Committee will oversee the development and maintenance of major initiatives, such as a disaster/recovery plan and a business continuity plan.

Most importantly, the Governance Committee is responsible for communicating risk issues and mitigation efforts with airport senior management. This communication is essential to maintain the needed level of support, and to ensure the viability of the committee itself.

The following list contains the overall objectives of governance:

- To promote consistency, productivity, and shared stakeholder expectations
- To produce quality deliverables using pre-defined practices
- To empower stakeholders with flexible practices designed to produce quality deliverables
- To establish baselines for procedural reviews and governance performance evaluations

3.3 Risk Management

Risk management of security systems involves a thorough understanding and analysis of the impact of breaches on the organization’s objectives, goals, and mission. Airport operators strive to put controls in place that will minimize disruption of service. Managing the expectations of the traveling public, tenants, and staff will also be an important element of addressing security system risk. Any risk event, such as a malfunctioning mechanical gate or breach of a building containing vital systems should be brought to the attention of the airport operator’s emergency response unit immediately. Any compromise of systems can lead to disruption in the business processes, thus producing substandard performance.

Risk management therefore, is the way an organization identifies, assesses, and controls threats to its profitability, security, and safety.

Risk management, in the case of the airport’s protection of vital security systems, should focus on the following key objectives:

- *Asset Assessment (Identification and Valuation)*
- *Risk Analysis (Threat and Vulnerability Assessment)*
  - *Identification of vital systems impacting airport security*
  - *Identification of threats and threat vectors*
- *Identification of mitigation strategies (Countermeasure)*

There are many different risk management methodologies to assist an airport operator, however, for the purposes of this guidebook, the CRAMM (CCTA Risk Analysis and Management Method) provides an approach that embraces the physical/logical/technical (e.g., IT hardware and software) and administrative nontechnical (e.g., physical and human) aspects of security and provides three effective stages for implementation:

STAGE 1 – ESTABLISHMENT OF THE OBJECTIVES

- Defining the scope for the Risk Assessment study
- Identifying and valuing the physical assets that form part of the system
- Determining the value of the data held by interviewing users about the potential business impacts that could arise from unavailability, destruction, disclosure, or modification
- Identifying and valuing the software assets that form part of the system

STAGE 2 – ASSESSMENT OF THE RISKS

- Identifying and assessing the type and level of threats that may affect the system
- Assessing the extent of the system's vulnerabilities to the identified threats
- Combining threat and vulnerability assessments with asset values to calculate measures of risks

STAGE 3 – IDENTIFICATION AND SELECTION OF COUNTERMEASURES

CRAMM, like other methods, is used as a tool to identify threats and select applicable countermeasures. Appendix B provides a matrix for both physical and logical controls and countermeasures. This matrix was created to assist the airport operator with creating a baseline of security controls for vital systems impacting airport security.

Two examples of the manual CRAMM assessment are shown in Tables 6 and 7. The process to create these example assessments are detailed in the Risk Management section of Appendix A.

Table 6. CRAMM Risk Assessment Example: Credit Card Data

Asset Owner: Sample Airport
Name/Department: SAMple Parking Operations Manager

Asset: *Credit Card Data*
Location: *Parking Data Room 231 (SAMple Airport Terminal Parking Deck)*
Description: *Credit Card Data is handled through various airport systems including the Parking Revenue System, The Shared/Common Use System, and the Finance Department's Merchant Account*

	CONFIDENTIALITY			INTEGRITY		AVAILABILITY	
	public (0) restricted (1–5) confidential (6–9) secure (10)			low (1–3) moderate (4–7) high (8–9) very high (10)		low (1–3) moderate (4–6) high (7–8) very high (9) mandatory (10)	
Impact Requirement *(1–10)*	10 / secure			10 / very high		8 / high	
Threats *list all that apply*	Disclosure	Theft	Loss	Hacking	Input Errors	Drive Failure	Power Failure
							Vulnerability (1–10)
none (0) *low (1–4) moderate (5–7)* *high (8–9)* *very high (10)*	10	3	1	8	2	5	2
							Threat (1–100)
Impact X Vulnerability = Risk Level	**100**	**30**	**10**	**80**	**20**	**40**	**16**
Low (1–33) *Medium (34–67)* *High (68–100)*	High	Low	Low	High	Low	Medium	Low
Countermeasures *list all that apply*	Password Protection Encryption	Physical Locks	Backup	Firewall	Data validation	Redundant Hard Drives	Backup Power
					Data Input Forms		

Table 7. CRAMM Risk Assessment Example Form: Access Control System

Asset Owner: Sample Airport
Name/Department: SAMple Parking Operations Manager

Asset: *Access Control System (ACS)*
Location: *Data Room 101 (SAMple Airport Terminal)*
Description: *The ACS handles all access to doors within the terminal and some outlying buildings. Other buildings not on the ACS are controlled by the Cardkey or with Keyed locks and have their own CRAMM form.*

	CONFIDENTIALITY			INTEGRITY		AVAILABILITY	
	public (0) restricted (1–5) confidential (6–9) secure (10)			low (1–3) moderate (4–7) high (8–9) very high (10)		low (1–3) moderate (4–6) high (7–8) very high (9) mandatory (10)	
Impact Requirement *(1–10)*	10 / secure			10 / very high		9 / high	
Threats list all that apply	Disclosure	Theft	Loss	Hacking	Input Errors	Physical Access to System	Power Failure
							Vulnerability (1–10)
none (0) *low (1–4)* *moderate (5–7)* *high (8–9)* *very high (10)*	10	3	1	8	2	8	8
							Threat (1–100)
Impact X Vulnerability = Risk Level	**100**	**30**	**10**	**80**	**20**	**72**	**72**
Low (1–33) *Medium (34–67)* *High (68–100)*	High	Low	Low	High	Low	High	High
Countermeasures *list all that apply*	Password Protection Encryption	Physical Locks	Backup	Firewall	Data validation	Add Locks to Data Room or Access Control	Install Backup Power
					Data Input Forms		

The CRAMM method can be utilized in-house at an airport by using the Security Officers Management and Analysis Project (https://www.somap.org) open source software titled ORICO (beta) as a desktop web-based client to run a full risk assessment. Additional free tools for risk management (some also have governance and compliance components) include:

STREAM – Acuity Risk Management (https://www.acuityrm.com/)

PRACTICAL THREAT ANALYSIS (PTA) Risk Assessment Tool – (http://www.ptatechnologies.com/)

GRC STACK – (https://cloudsecurityalliance.org/)

GLPI 0 – (http://glpi-project.org/spip.php?lang=en)

A full discussion of using Risk Management in action, including guidance on Risk Assessments as a part of the ConOps document, is included in Section 5 under Financial and Operational Considerations. *Recommended Security Guidelines for Airport Planning, Design, and Construction* states that "a key element of the ConOps for the development of an airport security system is a Risk Assessment, the principle components of which are a determination of threats and vulnerabilities" (Safe Skies 2017, 22).

3.4 Compliance

Compliance is a form of administrative control, whether it is adhering to local airport policies and procedures, federal and state regulatory compliances, or law. Those tasked with securing access to systems vital to airport security will want to familiarize themselves with both federal regulatory requirements and industry standards and best practices.

3.4.1 Federal Regulatory Requirements

Regulated commercial service airports must have an ASP in accordance with 49 CFR § 1542. Of course, every airport is unique and security measures vary from airport to airport. Every regulated airport must have a program under § 1542.103(a) and a supporting program under § 1542.103(b) to meet the regulatory requirements or provide for additional measures beyond those minimums outlined within this document. Each ASP is typically structured to reflect regulatory intent and requirements, as well as current airport amendments and Security Directives (SD). The ASP calls for an Airport Security Coordinator (ASC) under § 1542.3; however, § 1542 does not require a Governance Committee. Many airports have airport security consortia, typically chaired by the ASC.

Coordinating efforts between the various stakeholders requires strong management. For example, an SD change from TSA may necessitate modification of the ASP or implementation plans, while an Information Circular may not be required or specify a change to the ASP.

Section 5.6 explores the usefulness of capturing access controls and control types in the ASP and the creation of a Written Information Security Program/Plan (WISP) that the airport operator can use as an internal resource guide for the ongoing Governance, Risk Management, and Compliance surrounding security components on the airport campus.

Still at other airports, the airport designee is the chair of the consortia. In a large-hub airport in the south for example, the ASC is the chair of the consortia and chooses when the meeting happens (e.g., once a month) and stakeholders from the airport, tenants, airlines (with their own security program), TSA, etc. will meet to discuss issues. In another large-hub airport in the northeast, for example, the airlines will chair the consortia.

3.4.2 Applicable Industry Standards

There are many industry standards and best practices that are applicable to both physical and cybersecurity protection in airport systems. Many international organizations, such as ISO, the IEC, and the International Telecommunication Union (ITU) have developed standards for access and network control systems, including newer standards for cybersecurity, understanding that these systems are not connected to the larger internet network.

Several standing bodies based in the United States are working to narrow focus on standards affecting domestic organizations from an access control and credentialing view. These organizations help to provide frameworks designed to assist stakeholders in the following areas:

- LAN, Wide Area Network and Cybersecurity – NIST http://www.nist.gov
    - FIPS 201
    - ISO 27001
- ANSI http://ansi.org
- Security Industry Association http://www.siaonline.org
- Underwriters Laboratory (UL) www.ul.com
    - UL 204
    - UL 294
    - UL 1076 ISO 19794-2

3.4.3 Transportation Systems Sector-Specific Plan (TS SSP)

It is important to mention that airports are a part of the Transportation Systems Sector-Specific Plan (TS SSP) as set forth in Presidential Policy Directive 21, Critical Infrastructure Security and Resilience. Per the TS SSP, the sector's mission is to continuously improve the security and resilience posture of the nation's transportation systems to ensure the safety and security of travelers and commerce. The TS SSP vision is a secure and resilient transportation system to enable legitimate travelers and goods to move without significant disruption of commerce, undue fear of harm, or loss of civil liberties.

Maintaining and securing the airport's vital systems infrastructure plays an important part in the TS SSP. Managing the risk of damage or failure of the airport's vital systems is critical to ensure the TS SSP's vision. Airports can begin to mitigate these risks by identifying, assessing, and prioritizing the risks to their systems.

Overall, implementing programs described in this chapter for Governance, Risk Management, and Compliance is essential for a complete Governance Framework.

Section 5.6 contains guidance for maintaining and managing compliance in both the ASP and the WISP, including references to useful templates and guidance in Appendix A.

SECTION 4: SECURITY CONTROLS AND VITAL SYSTEMS

4.1 Introduction

According to the United States GAO in the *Federal Information System Controls Audit Manual*, the control environment is defined to "set the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; and the way management assigns authority and organizes and develops its people."

To further define security controls for the purposes of this guidebook, the SANS Technology Institute gives the following definition, "Security controls are technical or administrative safeguards or counter measures to avoid, counteract or minimize loss or unavailability due to threats acting on their matching vulnerability, i.e., security risk." (Security Controls Version 1.2, SANS).

The development of meaningful and enforceable controls can proceed once the airport has established a workable governing body through its governance process, and has established framework of policies procedures, standards, baselines, and guidelines. The purpose of this section is to delve further into the types of controls that are necessary, with illustrative examples, and to identify the most critical systems that are responsible for airport security and safety. It should be noted that the control examples listed are general in nature. Each airport organization will need to develop controls that are specifically tailored to its own operating environment.

As stated previously, the confidentiality, integrity, and availability (CIA) of security systems is the goal for asset and system management. It is through administrative, technical, and physical controls that the CIA Triad is achieved.

Though developing a fully evolved control framework may not be necessary for most airports, a thorough understanding of the reasons for a strong framework approach remain the same, irrespective of airport size. Per the $(ISC)^2$ CISSP Common Body of Knowledge, the need for a control framework is as follows:

1. **Consistent** – A governance program must be consistent and a common approach must be understood and applied by all elements of the airport organization.
2. **Measurable** – The governance program and controls must have measurable metrics to ensure that the controls are achieving the level of security that has been determined necessary.
3. **Standardized** – Controls should be standardized across all aspects of airport operations and be meaningful. Standardization is critical for controls to be measurable.
4. **Comprehensive** – At the very least, controls should cover all airport regulatory and legal requirements. They must reflect past and current board actions, where applicable.
5. **Modular** – A control framework that can easily be adapted to changing organizational environments is more likely to last over time. When controls are adapted for specific organizations, even the smallest organizational change requires a control rewrite. Controls should be adopted that reflect situations, not organizations.

Many government organizations use NIST's Special Publication (SP) 800-53r4 when developing a method for defining and categorizing controls. Though the NIST SP is specifically for federal government organizations, it is easily adapted to the airport environment.

The NIST SP lists the following 19 control families:

- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Planning
- Privacy Controls
- Program Management
- Risk Management
- Security Assessment and Authorization
- System and Communication Protection
- System and Information Integrity
- System and Services Acquisition

It should be noted that the NIST control framework corresponds to the ISO 27001:27013 standard, and airports may wish to use that standard as it has been adopted by organizations, such as the Airports Council International, which has a global perspective.

Whether using NIST or ISO, there is a potential for airport controls in every category once the airport control framework is fully established.

4.2 Developing Controls

It is important to understand the different control categories and how each may fit into an airport's own operating environment. It is often advantageous for airports to work with other airports to borrow controls that have already been established, and then modify them to fit operating circumstances and environments.

All controls may be categorized into one of the following seven types:

- **Directive –** Directive controls are designed to specify acceptable rules of behavior, e.g., an airport employee must wear their identification badge in a visible manner at all times.
- **Deterrent –** Deterrent controls are designed to discourage people from violating airport policies or directives, e.g., employees found "piggy-backing" on another's badge into a restricted area will have their credentials removed.

- **Preventive –** Preventive controls prevent a security incident or breach, e.g., an employee must have a password of greater than 10 characters.
- **Compensating –** Compensating controls are implemented to mitigate the loss of primary controls and reduce risk to an acceptable level, e.g., data backups will be performed daily on all airport workstations.
- **Detective –** Detective controls are designed to issue a warning when a security control has been violated or breached, e.g., an access controlled door alarm is sounded when someone goes through the door without using the access control system properly.
- **Corrective –** Corrective controls are created to mitigate damage, or restore controls, e.g., the immediate response by security personnel to an alarm on an access controlled door.
- **Recovery –** A recovery control seeks to restore conditions to normal after a security incident, e.g., an airport creates a policy that all access controlled doors are reviewed after one alarm is triggered.

The above controls are created relative to the timeline of a security incident, meaning that some are developed to prevent an incident (directive, deterrent, preventative and compensating) and the others (detective, corrective, and recovery) are created to act in response to an incident.

The 19 control categories (based on the NIST SP), and seven different types of controls have been further categorized based on the method in which they are implemented. There are three different ways to implement a control:

- **Administrative –** These are basically management directives in the form of policies, guidelines, and SOPs, and are usually carried out through management functions.
- **Logical/Technical –** These controls are implemented through hardware and software and typically are components of the airport's technology environment.
- **Physical –** These are for the protection of personnel and property—anything present in the airport's physical environment. Examples include locks, gates, perimeter intrusion detection systems, guards, bollards, etc.

While any department or stakeholder of an airport can create any type of these controls, they likely fall into the following categories:

- **Administrative:** Airport management, Human Resources, Legal Counsel, Airport Operations, Finance
- **Logical:** IT, Public Safety
- **Physical:** Public Safety, Facilities Management, IT

4.3 Examples of Controls

Table 8 illustrates controls in each category and for each type that could be developed to carry out this goal. This is far from an exhaustive list and is solely intended to provide examples of each. A more comprehensive example of security controls can be found in Appendix B.

Table 8. Control Examples by Category

Controls		Examples
Directive	Administrative	Airport employees may not share video images from the airport's closed-circuit television system without express written approval of the public safety department.
	Technical	Administrative passwords on all security systems must be changed every 30 days.
	Physical	"Do Not Enter without Authorization" signs are placed on the entry to all airport communication rooms.
Deterrent	Administrative	Employees found sharing their user identification and password with any other individual will have all system rights immediately revoked.
	Technical	When logging on to an airport physical security system, a warning banner is displayed that states only authorized personnel may attempt access to the system.
	Physical	A sign is posted on a controlled door that states only authorized personnel may enter and a violation that engages the alarm may be subject to criminal prosecution.
Preventative	Administrative	A policy that requires all contract personnel to be cleared through a background check process before being allowed to work on physical security systems.
	Technical	All airport communication rooms that house physical security systems must use both an automated access control mechanism (swipe card) and a pin.
	Physical	All physical security systems are stored in separate caged areas in the airport's data centers and the "least privilege" concept applies to access.
Detective	Administrative	All attempts to enter a restricted area with an unauthorized badge will be recorded in the system's security log and logs are reviewed at least weekly
	Technical	Detailed logs will be maintained for all physical security systems for a minimum of 90 days.
	Physical	CCTV will be employed at the entry to all data centers and communication rooms that house physical security systems.
Corrective	Administrative	Any airport employee found violating the badge use policy will be suspended upon first violation and terminated on any subsequent violation.
	Technical	Any desktop workstation that is suspected of containing malware will be immediately unplugged from the airport network and may not return to the network until it has been thoroughly investigated and "cleaned" by the IT department.
	Physical	A fire alarm will activate the airport's data center fire control system within 60 seconds if not overridden through human intervention.
Recovery	Administrative	The airport will maintain an updated disaster recovery plan at all times, with periodic testing no less than every six months.
	Technical	All physical security systems will have a backup schedule with a recovery point objective of no more than 4 hours.

	Physical	The airport will maintain a Disaster Recovery "hot-site" for all physical security systems that can be activated within one hour of a major disaster.
Compensating	Administrative	Badged airport personnel must escort all contract personnel when working on airport security systems.
	Technical	Facial recognition analytics will be employed at the entry to any physical security system.
	Physical	All security systems will be protected through multiple defense mechanisms, including locks, cages, and locked racks.

There are hundreds of different access approaches, control methods, and technologies, both in the physical and logical world. For example, solutions in the physical world may incorporate natural and man-made barriers while logical controls use identification and authentication mechanisms.

Access controls are necessary to protect the confidentiality, integrity, and availability of objects (in this case, the systems vital to airport security). The CIA Triad is applicable to all security controls, from the physical barriers protecting the airport's curbside to the 24/7/365 uptime of an Access Control System's server.

This section presents a categorization method of controls applicable to both physical and logical security. A layered defense-in-depth model includes providing control recommendations starting with policies and/or directives through deterrent, preventative, compensating, detective, corrective, and recovery categories. Table 9 illustrates the control categories and types.

Table 9. Control Categorization & Types

	Administrative	Technical/Logical	Physical
Directive	Policy	Configuration Standards	Authorized Personnel Only Signs Traffic Lights
Deterrent	Policy	Warning Banner User Access Policy Signature	No Trespassing – Electrified Fence Sign
Preventative	User Registration Procedure	Password-based Login 2 factor-authentication	Fence
Detective	Review Violation Reports	Computerized Logs Periodic Review of Access	Sentry CCTV
Corrective	Termination	Unplug, isolate, and terminate connection	Fire Extinguisher
Recovery	Disaster Recovery Plan	Backups	Rebuild
Compensating	Supervision Job Rotation Logging	Video Surveillance Keystroke Logging	Layered Defense

The table shows well-rounded examples of each category of security controls through the administrative, technical/logical, and physical control types. By using this approach, this guidebook presents the reader with the ability to focus on specific areas where they may need or require attention. The next section covers the vital systems that impact airport security. It is important to understand that access to these vital systems includes physical and logical access types; therefore, both mechanical and physical building structures are covered, in addition to computerized systems and networks. A comprehensive Security Controls Matrix is presented in Appendix B, blending the security control types above in Table 9 with the vital systems covered in the next section.

4.4 Security Controls

The key goal in protecting an airport's physical security systems is in ensuring that the CIA Triad is maintained at all times. It is important to take a closer look at these concepts and then apply each of them specifically to an airport's physical security systems.

CONFIDENTIALITY

Confidentiality ensures that only authorized individuals have access to systems and the data contained within them, and that those individuals have a "need-to-know," otherwise called the principle of least privilege. This means that every airport employee should only have the access necessary for them to do their job. This is not a particularly unique approach. Airports routinely restrict access to areas of the airport based on an employee's duties and role.

A critical component in determining access to systems is based on the data contained within them. This is typically conducted through data classification. Most physical security systems contain highly sensitive data, and should be classified accordingly. Video images from the airport's CCTV system may contain video recordings of events that are subject to law enforcement rules of evidence, or contain highly sensitive information that could end up in a criminal or civil court of law. Airport CCTV data may also be shared with federal agencies such as the TSA or Customs and Border Protection (CBP). In these cases, the video images likely fall under federal data classifications, in addition to the airport's own determinations.

When considering who may have access to physical security systems, it is important for the airport to consider all of the data maintained and carefully determine who should have access.

INTEGRITY

Integrity of data requires that the airport can provide assurance that the data contained within its systems has not been intentionally or unintentionally altered in a manner that invalidates the proper use of the data. All information should be gathered, stored, and disseminated according to commonly accepted business practices. Typically, integrity is easy to maintain if an airport has instituted the proper controls. However, if the data's integrity comes under attack for any reason, most likely because of a court action, proving integrity is very difficult without significant controls in place.

Integrity begins early in a security system's life cycle. Proper controls must be built into the system from its inception, tested thoroughly to ensure that they work as expected, and occasionally audited to prove ongoing compliance. For example, if a physical access control system's logs are used in a personnel matter as evidence of noncompliance with an airport's time and attendance policies, an accused employee may seek to discredit the information if there is any perceived flaw. Because judicial systems often do not have the expertise to delve into system processes, it is to the airport's advantage to be able to demonstrate that it has taken due diligence in developing the necessary system controls and has exercised due care in carrying them out so that any reasonable review will conclude that the system has maintained integrity.

AVAILABILITY

While both confidentiality and integrity are important in any technology system, perhaps availability stands out a bit more when discussing physical security systems. Physical security systems must be available 24/7, and loss of systems can cause significant issues for an airport. Loss of service can occur for any number of reasons. It could be a natural disaster (e.g., earthquake, flood, fire, or hurricane) or man-made issue (e.g., system crash, lack of adequate system resources, or cybersecurity incident). Whatever the reason, loss of service of a physical security system can potentially have costly and/or dangerous security consequences.

Particularly with physical security systems, redundancy, disaster recovery, and business continuity are critical planning tasks that must be carried out and maintained over a system's life.

When developing controls through the governance process for physical security systems, the CIA Triad provides the core security principles that must be achieved. Every control must seek to enhance the protection of one, two, or all three of these principles. For example, establishing a requirement for two-factor authentications for entry into a physical security system furthers all three principles. It keeps the information more confidential, lessens the likelihood of unauthorized manipulation, and helps to ensure uninterrupted service. Developing a system for the creation and storage of backup data likely only impacts the availability of the system.

Using the CIA Triad is an essential step in considering all aspects of the ramifications of developing airport security controls. Once it becomes an ingrained part of the decision-making process, an airport will find that it helps to guide development of security controls.

In the next three sections, controls are further defined as physical, technical/logical, and administrative.

4.4.1 Physical Controls

The protection of physical security systems should be considered part of the airport's overall physical security plan, with special provisions and mitigation efforts developed specifically for such systems.

Each physical security system should be established within a security zone that begins in the data center, where the head-end equipment is located, then to every communication room where network equipment is maintained, and finally to every end-point device. It may be necessary to include the connecting media (copper or fiber) if run through particularly vulnerable areas.

Within each security zone, a variety of controls must be considered to protect against natural and/or man-made threats. The following are physical security controls that should be considered:

- **Fire suppression** – This must account for protection of both the equipment and for any personnel that may be near the equipment should a fire or smoke incident occur.
- **Access Control –** Fail Safe (open) should be the policy on any controlled doors in case of a fire incident.
- **Access Routes –** Where possible, multiple access routes for personnel should be established in the event of any major man-made or natural disaster that threatens or impacts physical security systems.

- **Physical Protection –** Special consideration must be given to the protection of all physical security systems, beginning with the most secure data centers and communication rooms, and the special protection of end-point devices that are located in high-traffic areas or are easily accessible by potential bad actors.
    - For example, a CCTV camera located in a corridor with a particularly low ceiling should be covered with a protective covering to prevent tampering. Another example involves physical requirements for data centers and communications rooms, which may include reinforced walls, special barriers, man-traps, and cyber locks.
    - Physical security of Bulk Electric Systems (BES) are covered in detail through the NERC CIP-006-6 Cyber Security and Physical Security standards. These standards cover managing physical access to BES by specifying a physical security plan to be used against compromise that could lead to a malfunction or instability in the BES (NERC, 2014).
- **Contractor Access –** While it is common for airports to utilize third parties to manage and operate physical security systems, special consideration must be given when determining who, how, and when access is granted to contractor employees. The contract that governs the relationship between the airport and the contractor must include provisions for background checks, criminal records, suitability of character, etc. If these requirements are not included in contracts, the airport could easily be accused of not carrying out its due diligence and due care in the maintenance and management of the contract.

    Once the contract is in place, the airport must work carefully with contractor management to ensure that all contractual provisions, such as security provisions, are observed without question. Any violation must be immediately adjudicated, with termination of offending personnel the resulting action where it is found that the contract has been violated. If the contract violation pertains to the entire company, the airport must consider contract termination as the proper action, as severe and potentially disruptive as it may be.

Alternate physical controls include the concept of Crime Prevention Through Environmental Design, which starts during the design phase of facilities and physical spaces. Per ANSI/BICSI 002-2014 design and implementation best practices, there are three underlying principles:

- Natural Access Control
- Natural Surveillance
- Territorial Enforcement

Additional standards covering aspects of physical and environmental security are found in the NIST SP 800-14 standards, including physical access controls, fire safety factors, failure of supporting utilities, structural collapse, plumbing leaks, and more.

CBP’s *Airport Technical Design Standards* addresses the security needs of a physical location and the following environmental factors that should be taken into consideration:

- **Temperature** – Vital systems should be housed in temperature-controlled spaces and follow BICSI standards. These standards provide guidance on correct temperature and humidity settings pertaining to network equipment, servers, and stored backup media.
- **Water** – Water close to physical spaces where electronics and equipment is stored, such as outside enclosures, out buildings or water resource piping (plumbing), should be monitored for potentially damaging rising levels and/or breaks.

- **Dust** – Dust is a major threat to sensitive electronic equipment. Dust is found naturally in the air or may be introduced as a result of nearby construction. Internal construction using dry-wall is particularly damaging to computer equipment.
- **Vibration** – Airport buildings are prone to vibrations from the aircraft they serve; therefore, special attention should be paid to physical location. Whether it is discussing these factors with the IT department during ongoing operations or during the design phase of building, these issues must be addressed with proper design to ensure vital systems are not compromised unnecessarily.

4.4.1.1 Airport Systems and Network Access

Systems are composed of software and hardware. Likewise, networks consist of data traveling over physical wire or wirelessly. Using access control on physical hardware prevents threat actors from stealing, destroying, or extracting the data housed in the equipment.

Hardware found in a telecommunications room, rack, or space typically connected to a physical network includes:

- Servers
- Hard drives
- RAM/ROM
- Motherboards
- Switches/Routers
- UPS power supplies
- Racks
- Cable distribution
- Firewalls

The physical network also needs controlled access to items such as:

- Conduit
- Cable trays
- Above ceiling runs
- In-ground cabling
- Fiber and distribution boxes
- Exposed cable/fiber

4.4.2 Technical/Logical Controls

In the fast-moving space of technology, controls can have a hard time keeping up. Fortunately, there are many controls that aid and assist users in minimizing both risk to and vulnerability points of vital systems (see Table 10).

Technical innovations in networking have added significant functionality and flexibility, as well as complexity. Originally, networks existed solely to facilitate a communication path from point A to point B; function was the primary goal. Systems became more reliant on the network and more devices became TCP/IP capable; as a result, the network has become critical to organizational success and more complex to meet the evolving requirements. As the importance of the network has increased, network security also has become more relevant.

Table 10. Network and Systems Control Types

Control	Network (Active)	Application/Operating System (Software)
User Passwords and Authentication	All Areas	All Areas
Access Control List	Switches Routers Firewalls	
Network Admission Control (NAC)	Switches Routers Firewalls	Software Defined Network (SDN)
Remote Access	Firewalls Remote Access Appliance	Virtual Private Network (VPN) Software Application
Network Segmentation	Switches Routers Firewalls	Software Defined Network (SDN)
Defense in Depth	All Areas	All Areas

Network security started to present itself on the public edge of the organization in the form of access control lists (ACL), which controlled traffic across a point by IP address, and later by protocol ports. ACLs gave organizations control over traffic coming into and out of the network. As applications and attacks became more sophisticated, network visibility and control over traffic and data needed to adapt and become more sophisticated as well. This led to the current approach to network protection, contextual awareness, which is the ability to identify and act on communication attributes, such as who, what, when, where, and how, and make dynamic policy decisions at every access point of the network rather than just on the public access edge.

In airport environments, security systems are critical to the safety of the public. Network access to security systems, such as PIDS, badge access, and surveillance systems, should be tightly controlled, forming to the model of least privilege. Key network access controls to accomplish this include NAC, network segmentation and hardening, and remote access.

4.4.2.1 Network Admission Control (NAC)

NAC is a network security system that performs authentication and authorization of users or devices prior to gaining access to the network. This moves the security control point to every entry point of the network.

Traditional networks were protected by a single firewall as shown in Figure 6. Figure 7 shows an integrated network with control points at every entry point.

Figure 6. Traditional Network with Edge Firewall

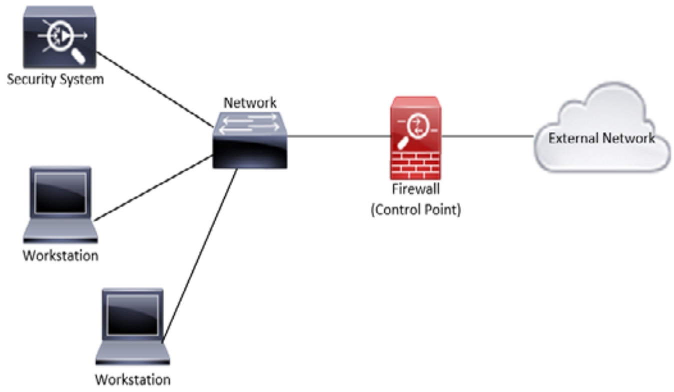
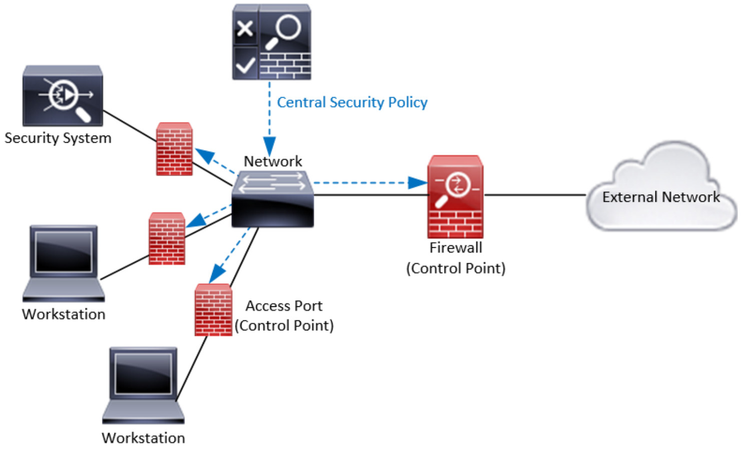


Figure 7. NAC Integrated Network



NAC is a crucial technology in providing identification and authorization requirements in many regulation standards, such as NIST and PCI. The key technology behind NAC is the 802.1x protocol, which enables a network device and endpoint NAC agent to communicate authentication, authorization, and contextual data to the policy engine. The policy engine is a system that is implemented to take business identity and access policies and enforce them across the entire network using the 802.1x protocol.

The central policy management allows security controls to be distributed across the entire network universally, reducing the risk of misconfiguration or noncontiguous security policies. This technology set is important for meeting identification and monitoring requirements set forth by NIST 800-53 in control numbers IA-2, IA-3, IA-7, IA-8, and IA-11 (DRAFT NIST Special Publication 800-63B, 2016). NAC is becoming more prevalent in most of the compliance and regulation standards, such as PCI 3.1 and Sarbanes-Oxley (Sox) due to its effectiveness. When used in conjunction with proper network segmentation and hardening, airports can provide true network resiliency and visibility.

4.4.2.2 Network Segmentation Hardening Practices

In many airports, security networks that facilitate the security systems have been physically separated to provide perceived security. Modern network technology makes physical network separation unnecessary.

“Organizations should create a network segmentation security model as soon as possible. While organic growth and the speed of business can make planning a challenge, the benefits are too great to ignore, according to Matt Gangwer, security operations leader with Rook Security.” (The Essential Guide to Securing Remote Access, 2016). Network segmentation is vitally important in new architecture models for Software Defined Networking (SDN), but it also plays a key role in network security for traditional network models.

Additionally, virtualization technologies allow parallel networks to work securely and efficiently on shared network hardware. This is major cost reduction in hardware procurement and support. Virtualization technologies include local area networks (VLAN), routing tables, and network devices. VLANs are logically separated networks that allow devices to be segmented into functional or criticality based groups and provides a control point between the group and all other devices. Virtual routing tables can be considered Layer 3 (Network Layer) zoning and allow groups of networks to be separated from other groups of networks on an IP routing level. See discussion in Section 4.4.2.4.

Virtual network devices take the previous technologies a step further by creating a separate network device in the hardware. The hardware resources such as network ports, memory, and CPU are assigned to the individual virtual instances, which are sometimes called contexts. The use of this modern technology practice reduces the overall attack vector that an airport might expose.

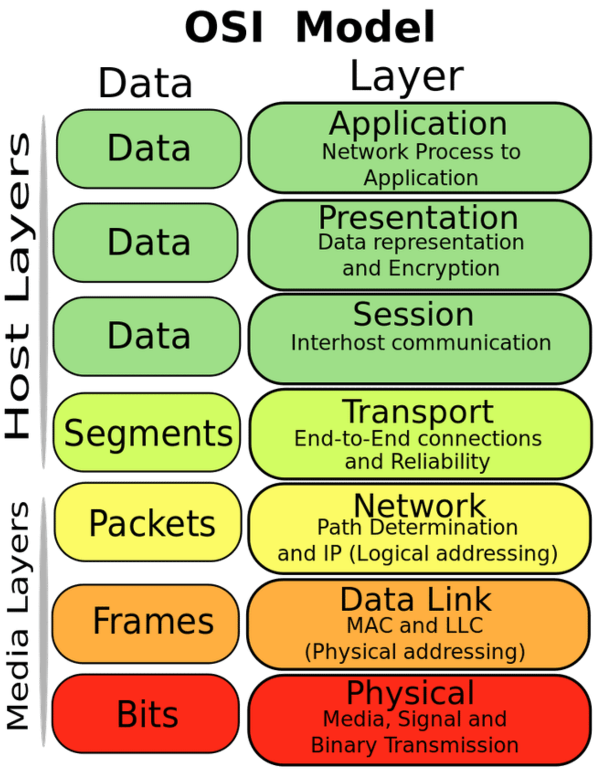
Another key security practice that airports should implement is to harden network devices per the vendor’s specifications. Hardening includes closing attack vectors by turning off unused services, protecting the device resources via the vendor’s provided security measures, and controlling access directly to the network device.

4.4.2.3 User Passwords and Authentication

Administrative controls help define the potential users of a system. It is a best practice to always encrypt user credentials when authentication occurs over a network. Rules should be in place to lock out users who fail consecutive login attempts, user sessions should be automatically closed after a defined period of inactivity, and default users should always be disabled, if possible. Additional best practices can be found in the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) checklists. These checklists are based on system type or manufacturer, and are available at https://www.stigviewer.com/stigs.

4.4.2.4 Access Control Lists (ACL)

Figure 8. OSI Layer Model


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data representation and Encryption
Data
Session
Interhost communication
Segments
Transport
End-to-End connections and Reliability
Packets
Network
Path Determination and IP (Logical addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal and Binary Transmission

ACLs provide a means for OSI (Open Systems Interconnection) Model Layer 3 devices to restrict or allow network traffic by IP address and protocols. Layer 3 is shown in Figure 8 as the Network Layer. Industry best practice is to explicitly deny all protocols and IP address ranges, and then stack rules to allow traffic as required by each application. ACLs can provide a means to deny access to unauthorized network devices, and should be used as in a layered-security design, although this method should not be used without 802.1x or MAC filtering, due to the ease with which an unauthorized person can anonymously monitor traffic on a network segment and spoof an authorized user's IP address.

4.4.2.5 Remote Access

Organizations have many external resources that need remote access, such as contractors, vendors, and remote employees. While remote access is important for many organizations, it presents an attack vector for potential bad actors. It is important to ensure that in all remote access solutions, the user is verified with authentication, and authorized only to access the resources the user needs. In the case of airports, it is highly recommended that no direct external access be given to the security systems environment.

The use of jump boxes and management stations should facilitate a connection from the airport administrative environment to the airport security environment. A remote access user can have access to a machine internally that has the appropriate access required into the security environment. The remote user should be properly identified, authorized, and secured before obtaining access to the jump box or management station. Some of the ways to secure remote access includes using two-factor authentication, contextual authentication controls, and/or device access controls.

Jump box technology consists of a secured, hardened, properly audited/logged computer used to gain access to specific secured networks and/or systems. They use strong authentication, typically do not allow internet browsing, are fully patched and use restricted user accounts. Most are virtualized.

Two-factor authentication is a method in which a user enters their username and password like a normal login, however, the user then provides a second, different form of authentication. If the normal login is a username and password, which is something they know, then the user must provide either something they have or something they are. Biometrics would serve as something the user is. Biometric authentication includes technologies such as facial recognition, retinal scans, and fingerprint readers. Something the user has would be a one-time password, which comes in the form of a token that typically has a frequently changing key. Another item that a user might use to fulfill the something-possessed requirement is a smartcard that has the user's information stored on it.

It is important to know that, per NIST 800-53, “SMS-based two-factor authentication is no longer considered secure by NIST standards, as SMS messages can be easily intercepted or redirected by remote attackers.” Contextual authentication controls also play a huge role in what the user will be authorized to do. Gathering data such as who the user is (name, IP address), where the user is (location), when the user is attempting to get access, and how the user is attempting to access the network are vitally important to providing the correct services to the user and providing security for the airport. The organization should also be aware of machine-level information. Airports should collect and act on device information such as software versions, firmware, patches, and security products installed/active. It is important to deny traffic from a malicious or infected machine regardless of the user.

4.4.3 Administrative Controls

Administrative controls are management directives and come in the form of policies, guidelines, and SOPs, and are usually carried out through management functions. Most often, Airport Management, Human Resources, Legal Counsel, Airport Operations, and Finance departments handle these types of controls; although, each department may produce their own internal directives as a way to adhere to the organizational administrative controls.

Administrative controls important to accessing vital system and physical spaces impacting airport security come by way of the following areas:

- Policies, procedures, and directives
- Onboarding
- Identity management
- Computer and internet usage policy
- Shared tenant services policy
- Third-party user access policy
- Badging and credentialing policy
- Key usage policy
- Preventative control measures
- Controls for detection and correction
- Controls for recovery

4.4.3.1 Onboarding (People)

During onboarding of new employees, the Human Resources department can implement an onboarding process, including the following:

- Completing online or paper forms
- Background checks and approvals
- ID badging and credentialing
- Training
- Creation of systems roles and responsibilities, e-mail accounts, and network access

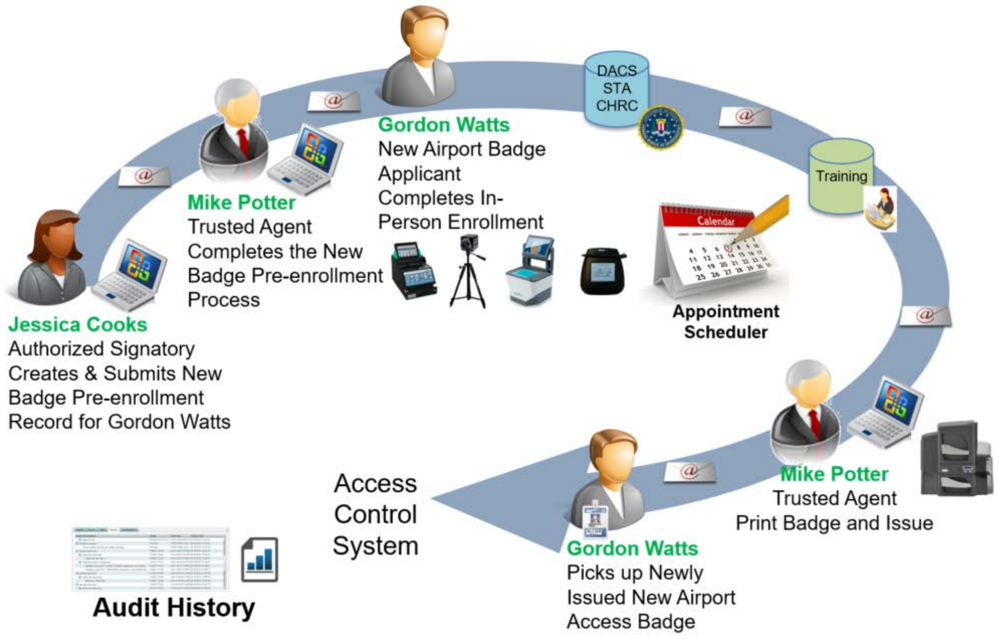
During the onboarding process, a control used by both Airport Operations and the IT department can involve overview of policies and procedures pertaining to accessing physical locations, computer systems, and the active/passive network infrastructure.

One airport authority surveyed sets up time with each department when a new employee arrives. The IT department can do a high-level review of their job responsibilities, the systems and people they support, and training on social engineering and how to use computers and systems per airport IT usage policies.

4.4.3.2 Identity Management (Badging and Credentialing)

Identity management and credentialing has become a vital part of the airport security system. ID badges are created based on verified information for an individual, and access types and roles are programmed to the badge. In the *Recommended Security Guidelines for Airport Planning, Design, and Construction*, credentialing is defined as "the process by which an individual is issued a credential that visually (and in some cases electronically) identifies the person as having been granted privileges for unescorted access to Secured and Sterile Areas on the airport" (Safe Skies 2017, 127) (see Figure 9).

Figure 9. Identity Management and Credentialing Example


Gordon Watts
New Airport Badge Applicant Completes In-Person Enrollment
DACS
STA
CHRC
Training
Mike Potter
Trusted Agent Completes the New Badge Pre-enrollment Process
Jessica Cooks
Authorized Signatory Creates & Submits New Badge Pre-enrollment Record for Gordon Watts
Calendar
Appointment Scheduler
Mike Potter
Trusted Agent
Print Badge and Issue
Access Control System
Gordon Watts
Picks up Newly Issued New Airport Access Badge
Audit History

Source: AlertEnterprise 2017

> *For example, a small hub airport surveyed employs a process for their air-gapped networks[2] to have remote access, only after the third-party vendor support personnel are verified on their list of supported users. Once verified, remote access is granted by physically connecting the internet to the air-gapped system and disconnected after the service has been performed.*

4.4.3.3 Computer and Internet Usage Policy

This policy is given to airport employees using computer systems and the internet to perform their job tasks. It covers areas such as acceptable use, personal use, confidentiality, and maintaining the corporate image. An example by the SANS Institute can be downloaded at https://www.sans.org/security-resources/policies/retired/pdf/internet-usage-policy.

4.4.3.4 Shared Tenant Services Systems Usage Policy

This policy is given to both airport employees and tenants using airport-based systems, such as a shared or common-use passenger processing system.

[2] An *Air-Gapped Network* is physically separated from the internet or an unsecured network

4.4.3.5 Third-Party User Access Policy

Remote and external access to computerized systems at airports has generally been given to both support staff and vendors who provide paid support and maintenance agreements. Depending upon the importance of the system to airport security, the controls can get increasingly narrow in focus. An example by the SANS Institute can be downloaded at https://www.sans.org/security-resources/policies/network-security/pdf/remote-access-policy.

4.4.3.6 Preventative Control Measures

Preventative control measures are performed daily at an airport for various types of inspections or audits (e.g., daily inspections of the runway to control foreign object debris or monthly inspections of airport maintenance fleet vehicles). The same attention should be given to systems and the physical spaces where those systems reside. Some preventative control measures include:

- Daily inspection reports and forms
- Supervisory auditing and controlling processes
- Asset management – keeping up to date with systems' physical locations, value, and any updates or changes made to the system that may impact airport security

4.4.3.7 Controls for Detection and Correction

Administrative controls for detection and correction of an incident are important for airports, if a legal event were to occur as a result of a breach to a system's security. The records surrounding an incident (e.g., video surveillance of a fence breach or attempted hacking into a system) are important to protect as they provide information pertinent to the detection of the incident and the corrective measures taken to resolve it. Some examples include:

- Records retention and disposal schedule
- E-mail and electronic file eDiscovery
- Forms used to record the incident
- Forms used to record the incident resolution

4.4.3.8 Controls for Recovery

After an incident has been detected and corrected, administrative recovery controls can help restore or rebuild. Having a good Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) will provide airport operators with the proper guidelines for recovery. Appendix B includes many examples of recovery for the systems and physical components addressed in this guidebook, and is a good starting point for an airport operator interested in creating a DRP and/or BCP.

4.5 Vital Systems

Many systems provide critical information to airport operators, staff, tenants, and passengers. This guidebook focuses on the systems that are vital to airport security. Special attention should be given to these systems during planning, design, implementation, active usage, and maintenance times. Attention should also be given to the systems' surrounding and supporting environments, from the communications networks they use to the physical spaces that provide protection from the elements and unauthorized access.

Although the asset and inventory assessment tasks in Appendix A will help airport operators create a list and assign a risk to each one, the initial list of systems, networks, and physical spaces should be vetted by the IT Department to ensure all systems have been addressed. Table 11 shows each of these vital systems and the airport security areas where they may reside.

Table 11. Vital Systems Used in Security Areas

Physical Location	Security Area	Vital Systems Used
Roadways	Terminal Campus Perimeter Inside SIDA/Secure NAVAID Access Roadways	Video Surveillance Access Control Systems
Perimeter Fence	Airport Campus	Fence-line detection Video Surveillance Pedestrian/Vehicle Gates Key Lock System
Internal Fence Areas	Airport Campus	Fence-line detection Video Surveillance Pedestrian/Vehicle Gates Key Lock System
Vehicle and Pedestrian Access Gates	Airport Campus Terminal	Access Control System
Employee Access Areas	Perimeter Gates Internal – Terminal	Access Control System Identity Management Systems
Terminal Lobby Areas	Ticket Counters Airline/Tenant Back Offices	Fence-line detection Video Surveillance Pedestrian/Vehicle Gates Key Lock System
Concourse Areas	Airport Operations Areas	Fence-line detection Video Surveillance Pedestrian/Vehicle Gates Key Lock System
SIDA/AOA Areas	Internal	Video Surveillance Access Control System Key Lock System
ID Badging and Credentialing Areas	Terminal External Building Location	ID Badging system Identity Management System

Physical Location	Security Area	Vital Systems Used
Telecommunication Rooms / Data Centers	Terminal Parking Garage	Video Surveillance Access Control System Key Lock System Identity Management System Biometric Access Control
Exterior Utility Rooms	Site and Terminal	Access Control System Key Lock System
Utility and Telecommunication Paths	Site and Terminal	Access Control System Key Lock System
Airport Operation Center	Terminal	Access Control System Key Lock System Biometric Access Control
Curbside	Terminal, Airline offices	Video Surveillance System Key Lock System Biometric Access Control
FAA NAVAIDS	SIDA/AOA	Access Control System Key Lock System Video Surveillance
FAA Control Tower Sites	SIDA and Terminal	Access Control System Key Lock System Video Surveillance
Fuel Storage Facility	SIDA	Access Control System Key Lock System Video Surveillance
Air Carrier Aircraft Parking Areas	SIDA and AOA	Access Control System Key Lock System Video Surveillance
Mail & Cargo Area	SIDA and Airport Campus	Access Control System Key Lock System Video Surveillance
Vehicle Parking	Terminal, External Building Location	Access Control System Key Lock System Video Surveillance
Aircraft Rescue & Fire Fighting	SIDA and Airport Campus	Access Control System Key Lock System Video Surveillance

Physical Location	Security Area	Vital Systems Used
Security Operations Center	Terminal	Access Control System Key Lock System Video Surveillance
Intermodal Transportation Facilities	Terminal and Landside	Access Control System Key Lock System Video Surveillance
General Aviation Parking Areas	SIDA and AOA	Key Lock System Video Surveillance
Baggage Claim Areas	Terminal	Video Surveillance
Security Checkpoints	Terminal and Sterile Area	Video Surveillance Law Enforcement Human Security (TSA)
International Arrivals Area	Terminal and Sterile Area	Video Surveillance Law Enforcement Human Security (CBP)

4.5.1 Premises Distribution (Wiring and Backbone Systems)

The physical portion of the network is typically called the structured cabling system or passive infrastructure, and it allows for the interconnectivity of all airport-wide communications systems. This interconnectivity is accomplished using fiber optic and/or copper cabling routed between each of the communications rooms throughout the airport's premises. The communications rooms serve as the distribution points for the end-users of various airport systems and peripherals.

Examples of such airport systems and peripherals include telephones, courtesy phones, pay telephones, multi-user flight information display system monitors, LED monitors, Common Use Terminal Passenger Processing (CUPPS) terminals, building management system control units, administrative network workstations, wireless access points, information kiosks, etc. These systems are served from the communications rooms; therefore, it is good practice to properly account for the collocation of these systems when planning cable routing, component placement, power, cooling, and similar future requirements. The cabling routed between communication rooms is known as backbone cabling, whereas the cabling to user workstations is station or horizontal cabling.

4.5.2 Data Center and Associated Hardware

The data center is a facility used to house computer systems and associated components. It generally includes environmental controls (air conditioning, fire suppression, etc.), redundant/backup power supplies, redundant internet connections, and high security.

4.5.3 Remote Access and Virtual Private Networks

In virtual private networks (VPN), which is the equivalent of a closed user group, users are grouped together by some common characteristics over a common domain. This network can run on dedicated equipment or through a shared infrastructure provider such as a telecommunications company. A VPN provides a secure environment that allows individual groups of users to share data and provide remote access to systems residing on a LAN. VPN appliances can be tightly coupled with network firewalls to provide access rules, authentication requirements, and granular user privileges in an effort to limit unnecessary exposure.

4.5.4 Network Security Management

An airport should implement layered security solutions with firewalls and intrusion protection systems at the edge of and inside the network. The airport should also implement industry-recommended practices for virus protection and patch management. Security typically already exists at a device level (e.g., workstation), application level (e.g., log-on password), and at a network level. The most vulnerable parts of a network are the interconnections, whether they be VPN connections or wireless access points. Good network design and careful management will mitigate intrusion and unauthorized entry.

Third-party companies can assist in the intrusion-detection arena. It should also be noted that physical security plays a large part in the overall network security plan. Networking equipment should be located in rooms that are physically secure.

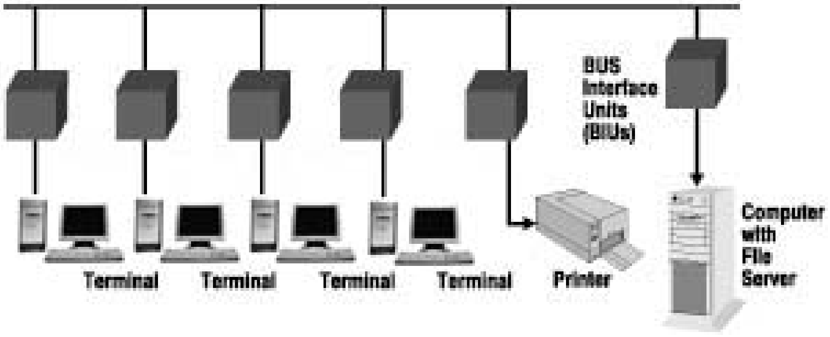
Network management can be either reactive or proactive. Reactive means that a user reports a fault and then a technician is dispatched. Proactive means that the IT asset is monitored and the watching agent intervenes without a user calling in the fault. This requires defining an operations support model with links to customer and vendor service levels. A wide variety of vendors offer incident management systems.

4.5.5 Local Area Network Systems

A LAN consists of a group of computers and associated devices that share a common communications line (wired or wireless) link back to a server. The LAN was created to share resources between computers such as printers, faxes, and general data from software packages (Figure 10).

Airports, like any other organization, use the LAN to bridge gaps in communications and data of all types, including security sensitive data such as access control and video surveillance information. As such, separation of duties, roles and responsibilities, and security must be implemented on the network and the systems that use it to exchange information.

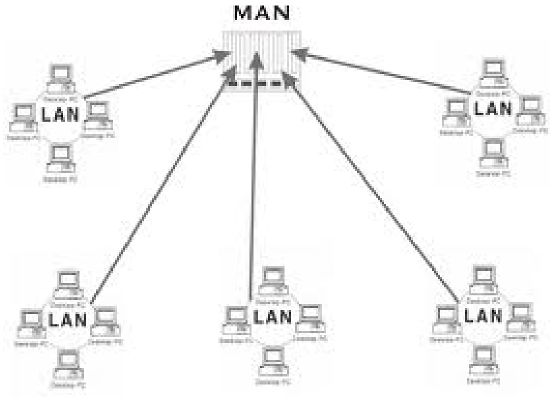
Figure 10. Local Area Network



4.5.6 WAN/MAN

A metropolitan area network (MAN), as shown in Figure 11, is a computer network larger than a LAN, covering an area ranging from a few city blocks to an entire city, possibly also including the surrounding areas. The wide area network (WAN) provides the connectivity from the LAN on a campus to points outside the campus, such as data centers located in other cities. Typically, today's WANs use technology similar to LAN-based switches.

Figure 11. Metropolitan Area Network



However, a WAN connection, unless properly configured and managed, could introduce delays and instability, which could affect the user through the reliability or latency of a connection. Airports do not generally have to develop WANs, as most of their applications and systems will only communicate at the campus-level through the LAN.

Wi-Fi is an extension of a wired Ethernet network that uses the FCC-allocated, unlicensed frequency band. As Wi-Fi is part of the wired Ethernet network, the same security, addressing, and design considerations can be applied. Multi-frequency antennae are used in the wireless distribution system as the connection point from the wireless portion of the network to the wired portion. The placement of antennae needs to be carefully coordinated during design and implementation to adhere to propagation study recommendations and to ensure adequate coverage. The wireless spectrum is very constrained and requires careful management to ensure that all systems using the wireless frequencies are configured for interoperability. An airport will need to consider how the spectrum can be policed and used efficiently. Third-party companies can perform radio propagation surveys, or alternate methods can be used to develop a radio map of the airport. Consideration should also be given to interference and its impact on airport radio operations.

4.5.7 Physical Storage Devices

Physical storage (mechanical or solid state hard disk storage/drives) is the repository for data from all systems. Over time, the data might accumulate without the proper controls in place. While the Security Information and Event Management (SIEM) systems manage the data and analytical uses of it, physical storage is required to keep the SIEM data in a suspended state until it is accessed again. The Radio Technical Commission for Aeronautics (RCTA) Standards for Airport Security Access Control Systems document provides useful definitions of storage types, including Direct Attached Storage (DAS), Network Attached Storage (NAS), and Storage Area Network (SAN). While each technology has its pros and cons, it is important to remember that unauthorized access to these systems could result in data being stolen or copied.

DAS, where the storage device is attached directly to a workstation or local server, is only suitable for small systems or systems where sharing video over a network is not planned. PCs with internal and/or external storage drives are common examples of DAS.

DAS devices are not network appliances but the data they contain can still be shared among multiple computers that have shared ports. Redundancy and fault tolerance depend on the hosting workstations.

NAS devices, as the name implies, are designed for sharing video across a network. NAS devices are network appliances that act as file servers and contain file-sharing software, and may contain multiple disk drives including RAID drives (see below). Network video recorders are examples.

SANs are network appliances that provide dedicated storage for enterprise-level networks where access to individual storage devices is important. Redundancy and recovery are enhanced by the ability of a SAN to span multiple storage arrays across physically disparate locations.

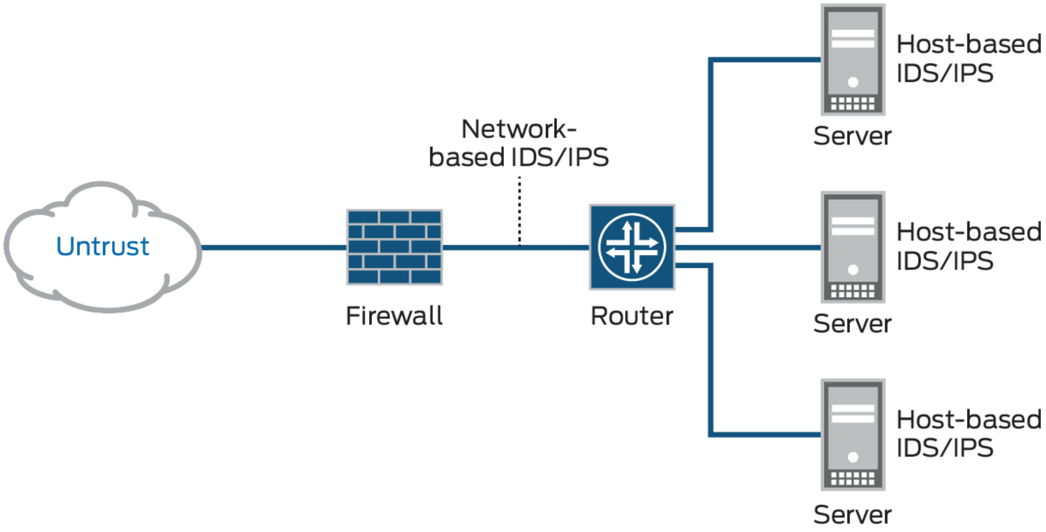
4.5.8 Network Intrusion Detection and Prevention

Intrusion detection and prevention systems (IDS/IPS) provide a means to mitigate the risk of unauthorized communication across the airport's enterprise network. This is commonly achieved by analyzing network traffic against threat signature databases, which require consistent updates, like host-based antivirus suites. Alternatively, a heuristic-based algorithm can be implemented in an effort to alarm on anomalous network traffic behavior. Once a signature is matched or anomalous behavior is identified, the system responds by notifying operators, in the case of Network Intrusion Detection systems, or blocking traffic, in the case of Network Intrusion Prevention systems.

Due to the risk of impact to critical operations, Network Intrusion Detection systems are initially deployed prior to a Network Intrusion Prevention system. Many commercially available solutions allow IPS hardware to initially run in IDS mode for a time period, which provides a baseline of behaviors and common network traffic types. This baseline can then be compared against new traffic patterns and anomalies, with a lesser risk of false positive alarms and possible disruption to service.

There are two major categories of IDS/IPS—Network and Host-based—as shown in Figure 12. Network-based solutions monitor application protocol activity, and sometimes behaviors, across a network or segment. Host-based solutions monitor the characteristics of a single host, and the events occurring within that host (Juniper Networks 2016).

Figure 12. Example Juniper Networks IPS/IDS Diagram



Management access to the IDS/IPS should be treated similarly to any other critical network component, following industry best practices and protocols to mitigate the threat of unauthorized management access, monitoring, and system modification. Out-of-band (OOB) management[3] for network-based IDS/IPS devices should be performed for remote access, allowing for continued and segregated access during an in-band intrusion event.

Using OOB management gives the IT department leverage to remotely access vital networks and systems during an intrusion event. It is important to document the OOB management methods, hardware and/or software components used when securing access to an airport's vital systems. Although OOB is a technical control providing an alternate access method, the OOB system itself should be documented using the Asset Management practices in this guidebook.

Physical access to system components should be restricted by storing network-based IDS/IPS devices in secure locations that are monitored by CCTV with all ingress/egress points under physical access control.

4.5.9 Physical Access Control Systems (PACS)

A PACS is a networked system of servers, software, computers, electronic card readers, identification access credential cards or tokens, intelligent field panels, magnetic or electric locking hardware, sensors, and interconnect cabling. A PACS may also include a mechanical lock with a conventional key.

Identification access cards are provided to the user with access levels authorized by the system administrator. These levels allow the card holder to access the appropriate PACS-controlled portals.

The PACS software provides event logging (typically for a minimum of 30 days), the ability to add and remove users and change their access levels, and data updates to the intelligent field panels and associated modules.

The PACS provides an airport with a standards-compliant system for controlling and monitoring access of people crossing areas of differing security levels. It also provides airport personnel with information needed to securely operate, enforce, and review airport security operations.

The PACS is typically a centrally controlled system with a primary server and hot standby server. The server transmits access information for doors, gates, etc. throughout the airport via PACS Data Panels. These panels store cardholder access data and communicate with devices at each door location.

Airport security operators interface with the PACS server from badging and alarm workstations, where operators can add new cardholders to the system, issue IDs, and maintain cardholder information. At alarm workstations, operators use PACS data to monitor door conditions and dispatch and coordinate with Airport Police when there is an incident.

Accommodations must be made to secure vital assets in the event of an extended power failure, during which traditional electronic PACS may fail to secure the facility. Additionally, an override function to allow emergency access to the asset needs to be considered for the case of an electronic malfunction that would prevent the normal operation of the PACS.

The access control system regulates staff and vehicle access to Secured and Sterile Areas throughout the facility. A computer-controlled access system is used at the necessary doors and portals. Not all doors and portals need to be covered by such a system; non-automated mechanisms can also be used.

[3] *OOB Management* is an alternate access method to vital systems, not connecting with the normal "in-band" network

The selection of monitored doors and those handled by other means is the responsibility of the Airport Police and security officials. Biometric readers or two-factor authentication (e.g., card plus PIN) readers are recommended for controlling access to sensitive areas. The readers should archive information on failed access attempts as well as passed authentications. Some access control systems have the capability to integrate with CCTV systems to bring up a video feed for a particular alarm; systems with this kind of technology should be considered.

4.5.9.1 Identification Badges

ID badges are an important part of the overall ACS because they are a system component that employees carry with them at all times to gain access to secure areas across the airport facility. The badge system contains a database of cardholder data and access privileges. The ID badge is also typically used as a visible indicator of access privilege (e.g., one color badge may mean the wearer has access to the AOA and another may indicate the person has access only to the terminal).

A badging printer has security features that make it difficult for anyone to forge an airport ID. Identification access cards are provided to the user with levels authorized by the system administrator. These access levels allow the card holder to access the PACS controlled door.

The ID badges and card readers may use secure smart card proximity technology. Smart cards and card readers should comply with the latest FIPS 201, TWIC, and TSA standards. Biometric technologies can also be utilized in addition to typical card and keypad input.

4.5.9.2 Biometrics

Biometrics is a means of capturing data about an individual (e.g., a fingerprint, face geometry, iris, etc.) A biometric device will use the IT and security infrastructure to pass a file from the point of collection to a local or remote system that compares the biometric to a database and takes action according to the software in use.

4.5.9.3 Card Readers

Card readers must be compatible with and read the ID badges used at the airport. Current card reader technology includes ISO 14443 and FIPS 201/PIV compliant, high frequency 13.5MHz contactless smart card technology, tamperproof, with mutual authentication and secure identity object encryption using OSDP[4] transmission protocol. Card readers should provide audible/visual feedback to the user, such as LEDs and a beeper.

4.5.9.4 Request-to-Exit Devices

Request-to-exit devices may be needed to shunt a door position switch and to send a signal to the PACS to unlock the door for authorized egress. Door position switches are used to detect when the door is held or forced open.

Request-to-exit device types include an infrared motion sensor, push button, and panic bar with integral switch. Motion sensors do not require action by the user; however, panic bars and push buttons do require action. The use of motion sensors to unlock mag locks from the secure side is discouraged

[4] **OSDP:** Open Supervised Device Protocol

because they can be easily defeated from the unsecured side by slipping something under the door, or other means to create motion/heat that triggers the sensor.

4.5.9.5 Electromechanical Mortise Locks

This type of lock is installed by hollowing out a cavity of the door along the leading edge and inserting the lock mechanism. A transfer hinge to allow wires to pass through is required to route power and data to the lock. The lock mechanism latch bolt is thrown into the strike. Electromechanical locks can be provided as either fail secure (locked during a power outage) or fail safe (unlocked during an outage).

These locks are considered highly secure because the lock is concealed within the door and difficult to access. This is especially true when the latch bolt is equipped with a latch guard that prevents movement of the latch when the door is in the closed position. These locks can be equipped with standard keyways that mechanically unlock the door, where an alarm could be generated via a separate door-position switch.

Control of the lock can be in one direction or both directions, or per other lockset function type. Electromechanical locks can control access in one direction through a card reader, and allow free mechanical operation in the other direction. If the access control card reader is located on the side of the door in the opposite direction of egress, there will not be a life safety conflict since egress is always available mechanically, such as by turning a lever or pushing a crash bar. These types of locks have moderate capital and operational cost.

4.5.9.6 Magnetic Locks

Magnetic locks are fail safe. An additional device, such as a card reader, request-to-exit push button, or motion sensor is needed on the secure side of the door to unlock the door.

Magnetic locks offer a high level of security due to their holding force (upwards of 1,200 lbs), but they also may provide the lowest level of security since they are inherently fail safe. These types of locks do not allow for bypassing the door via a mechanical key, and do not utilize any type of lockset function. Where a door is controlled electronically with magnetic locks, it is either locked in both directions or it is unlocked in both directions. Many Authorities Having Jurisdiction (AHJ) and life safety codes may not allow magnetic locks within the egress path. When magnetic locks are allowed to be used within the egress path, they are typically configured with a delayed egress function authorized by the AHJ or provided with overrides that can significantly reduce the level of security. Capital costs of magnetic locks are moderate, and the long term operational costs are the lowest of all types of locks.

4.5.10 Video Surveillance Systems

A video surveillance system is a solution that provides the means to monitor, record, and manage cameras and associated video. Typically, these systems are composed of application servers, network video recorders, storage devices, and client interfaces. Cameras provide encoded and compressed video streams to application servers and video recorders, so video can be archived and made available for live viewing through the client interfaces. Client interfaces are commonly desktop applications or web interfaces.

These systems provide a means for granular access control based on hierarchical or object-based classification of users, including restriction of camera groups, archived video, or time schedules. It is a best practice to associate minimum access (least privilege) to each user credential. User authentication services (e.g., Microsoft Active Directory Servers) are typically integrated with video surveillance systems to reduce the maintenance overhead. Privileged user account access should be consistently reevaluated.

System user interface terminals should be located in secure areas, out of view of public traffic to avoid unnecessarily disclosing camera locations and fields of view. These terminal operating systems should also be locked when unattended.

Video recorders, video storage, and management servers should be housed in secure areas, under physical access control and monitored by CCTV. Access to these critical components should be minimal, and collocating hardware with other systems that may need maintenance by non-privileged surveillance system users should be avoided. When not in a secure environment, communications infrastructure should be enclosed within conduit or armored cable, without publicly-discernable markings to identify it as security infrastructure.

Digital and analog cameras are a primary component of a video surveillance system. Each camera within the system must be selected based on its unique application and environmental conditions. There are many different types of cameras available on the market today, but they primarily fall into one of the following four categories: fixed, PTZ, panoramic, or multi-sensor. Cameras can be hardened or placed within an enclosure to mitigate unauthorized access, dust ingress, vibration, water ingress, overheating, explosions, or under-temperature failures.

Cameras placed within access of public foot traffic should be vandal-resistant, impact-resistant, and support active-tampering alarms that alert on events recognized as intentional blocking or spray-painting to obstruct the camera’s field of view. In some cases, where concern over tampering exists, conduit is run directly into the camera’s enclosure, and cables terminated within. Camera power and communications cables should be armored or enclosed in conduit.

4.5.11 Perimeter Intrusion Detection Systems (PIDS)

The purpose of a PIDS is to detect unauthorized access to areas identified by the airport as part of the SIDA, AOA, Sterile Area, or adjacent to critical infrastructure. In order to protect key assets, employees, passengers, and operations, an intrusion must be detected early enough to allow an appropriate response. The SIDA boundary is typically the first and preferred line of detection, providing as much time as possible for responders to verify and respond to perimeter security breach events. A PIDS solution is composed of tightly-integrated sensor subsystems, commonly using a layered security approach in a way that limits nuisance alarms, provides visual monitoring of events in real-time, and has a high probability of detection.

It is common to have sensor systems that are visible and sometimes accessible to the public. In these cases, edge devices should be vandal resistant, infrastructure enclosures should have interlocks that alarm when breached, and communications cable should be armored or enclosed in conduit. When locating sensors along the SIDA perimeter, special consideration must be made to avoid providing an unintentional fence climbing aid. PIDS are commonly integrated with Physical Security Information Management systems, and all interface points should be evaluated for placement under access control and monitored by CCTV.

Example sensor systems that are typically used in a PIDS solution include:

- Electronic Scanning Radar (solid state)
- Mechanical Scanning Radar (solid state)

- Fiber Optic Fence Detection
- Buried Cable Detection
- Laser Detection
- Thermal Cameras
- Infrared Detection
- Microwave Detection
- Culvert Detection
- Robotic Detection
- Mobile Detection

4.5.12 Airport Communication Systems

Airport communication systems connect stakeholders to one another, allow users to access their applications and business systems, and transport data, voice, and video from one point to another throughout an airport campus. Planners should keep in mind the OSI model, the use of IP addressing schemas including IPv6, directories, and user domain management. The communications systems should meet the business and technical objectives defined and articulated in the airport's IT Master Plan, which are aligned with the airport's overall business goals.

4.5.12.1 Integrated 800 MHz Trunked Radio, Land Mobile Radio, TETRA, IPICS Radio Systems

These systems allow users to communicate via walkie-talkie type radio, i.e., direct, device to device(s), usually over a short range—0.5 to 5 miles, depending on the power of the system and the environment. Complex user groups can be set up for a single user to monitor and communicate with multiple user groups to satisfy specific operational parameters. Often at an airport, the operational radio system will be part of a larger system that is sponsored by a city or county. In these instances, the airport portion of the system must abide by the standards established by the governing body. IPICS[5] will allow interoperability of radio with IP and other data networking protocols so that command nets may be set up in the event of emergencies or other operational incidents, supporting interoperability and communication between airport and metropolitan or state, civil defense, and military networks.

4.5.12.2 Centrex and Private Branch Exchange (PBX) Phone System

"Centrex is a voice telecommunications service that offers traditional telephone system features and functions often found in premises-based systems such as PBX [Private Branch Exchange]. Centrex is perfect for multiple-location businesses wanting a single, easy-to-use service." (AT&T 2017).

No switching equipment is present on the premises, and service is managed directly by the phone company at their exchange site, with physical lines being delivered to the customer's requested locations. Centrex provides the hardware of a PBX system through software emulation and can be programmed to meet the customer's needs. The PBX, by providing Customer Premises Equipment voice services, has been the industry-dominant system over the last several decades.

[5] **IPICS:** IP Interoperability and Collaboration System

4.5.12.3 Voice over IP (VoIP) or Wi-Fi Phone System

VoIP technology treats a voice call as a data transmission. The voice is received, converted to a "packet," and transmitted over a data LAN instead of through a PBX system matrix. When a call is sent to a location internal to the LAN, it stays under the control of the data network. When a call is sent to an external location (off the LAN), the call is routed to an outside line or trunk.

This is essentially a wirelessly connected IP mobile handset using 802.x, thereby using and interfacing with the airport campus network and operating accordingly. Integration with both the Wi-Fi component of the LAN and the telephone system must be performed to effectively configure a voice-over Wi-Fi telephone solution. It is important that this solution is coordinated and planned with the design and configuration of the Wi-Fi system to ensure that appropriate bandwidth and Quality of Service are provided.

4.5.12.4 Neutral Host Distributed Antenna System

Each airport should have a specific method and plan for accommodating cellphones. This method and plan should accommodate usage by airport staff, tenants, and the traveling public. A technical solution must be implemented to support the chosen business model. This should include accommodations for cellular carriers and their required equipment and distribution systems (cell sites, antennae, etc.), and performance of radio propagation studies. It may also include an in-building Distributed Antenna System either airport-owned or third-party provided, that handles traffic to all wireless phone carriers.

4.5.13 Airport Operations Systems

Airport Operations Systems are important to the safety and security of the airport in that they may support the backend data supplied to security systems. These systems often contain the correlating data used in passenger processing, PACS, video surveillance systems, and PIDS. Any downtime in these systems would impact airport operations such as processing passengers, allowing properly credentialed people access to secured locations, or baggage handling and routing.

4.5.13.1 Airport Operational Database (AODB)

The Airport Operational Database (AODB) system is the primary holder of all data that relates to operational activity, both flight and facility related. This database supports the real-time warehousing and retrieval of data from IT systems, and provides the platform and mechanism for the integration of systems throughout the campus. An AODB integrates into other airport systems and receives data feeds from outside sources, such as airlines (e.g., receiving IATA EDIFACT information). Typical data that the AODB will store includes which aircraft arrived when, from where, and departed bound for where, with how many passengers and how much freight, where it parked, and what other airport services it used. The AODB will contain historic, actual, and planned data, and feed enterprise and financial systems. The database can also drive other systems, such as Resource Management Systems, dynamic signage, etc., as well as feed airport enterprise systems for purposes such as billing.

4.5.13.2 Resource Management System

Resource Management Systems are key to effective planning for airport operations, especially as a facility reaches capacity. Examples of critical assets that affect an airport's capacity include fire cover (a function of the number and type of fire engines), runway capacity, stand or gate capacity, passenger concourse standing capacity, number of check-in desks, and number and size of security posts. Underpinning every resource management system is its ability to capture and manage flight schedules.

This is the activity around which the airport revolves, as well as a major source of income for specific airports. Real-time updates of this information feed the FIDS. A resource management system should also allow users to identify and create their own constraints, and define the business rules affecting these constraints.

4.5.13.3 Gate Management System

Gate management systems assign and allocate passenger and freight flights to specific gates, catering for remote stands, jetways, gate lounges, buses, and other services. Gates can be common use (shared) or dedicated (assigned to one airline).

4.5.13.4 Common Use and Shared Use Systems (CUSS, CUPPS, CUTE, DCS)

A wide variety of self-service kiosks are available. Those for airline check-in may be either dedicated or common use. Kiosks also support programs such as CLEAR and US Visit. Determining an effective location for a kiosk is both an art and a science, and this aspect should receive consideration, including the modeling of an airport's passenger flow based on different arrival rates. Kiosks require data ports and electricity, so their potential locations need to be well planned. Retailers may also use kiosks for selling snacks, newspapers, or other sundry items. Some kiosks are able to print baggage tags and an airline may want the airport to provide a fast bag-drop area nearby. A similar facility may be required to support off-airport baggage and passenger check-in (affiliated hotels or conference facilities). IATA has defined a CUSS Recommended Practice (IATA RP 1706a) for airlines to develop and deploy applications on shared kiosks that allow passengers to check in. Usually, an airport airline club owns a set of common-use kiosks and can determine their usage and associated fees.

Additionally, a common or shared-use system would involve the provisioning of a shared airport operational desktop platform that supports all airlines on a single set of common devices including workstations, boarding pass and ticket printers, bag tag printers, boarding gate readers, and others. This allows flexibility in the allocation of airport resources (ticket counters and gates) to individual airlines. CUPPS may also include IP telephony configuration for the user airlines, and may extend to Gate Information Display Systems (GIDS) and other airline signage systems.

The IATA Recommended Practice 1797, known as Common Use Terminal Equipment (CUTE), was introduced in 1994. While it defined the functional requirements of what a CUTE system should do, it did not provide any technical specifications that defined how airlines' check-in and boarding applications should communicate with peripherals such as boarding pass printers, bag tag printers, and boarding gate readers. As a result, various common use platform providers introduced their own version of CUTE, each with their unique Application Programming Interface (API). Airlines therefore had to develop different versions of their applications, one for each CUTE platform.

An airline uses a departure control system (DCS) to board passengers (i.e., assign them a seat and redeem the ticket voucher). Usually an airline DCS is a remotely located host application requiring either ALC, X25, or IP connectivity via a gateway. A DCS also provides an airline with the legal weight-and-balance data required for flight operations.

4.5.13.5 Baggage Handling System

Of all airport ground systems, the baggage handling system is probably the most passenger critical, since it is responsible for distributing bags from check-in to the aircraft gate loading area, and from the aircraft to the arrival belt, as well as facilitating transit bags. If it does not operate properly, flights cannot depart on time and passengers cannot complete their journeys. Furthermore, the size and complexity of the baggage handling system is driven by the number of airlines, the airport baggage handling area layout, and other factors that must be taken in to consideration when planning secure access methods and applications.

4.5.13.6 Airfield Lighting Control System

Airport lighting is so complex it requires an IT overlay. An airport lighting control system can control lighting from one or more locations, remotely monitor the proper functioning of the system, and automate many functions. More advanced systems will often be integrated with a surface movement guidance and control system.

4.5.13.7 Identity Management Systems

Identity Management Systems (IDMS) are used at airports to manage individual identities and the corresponding authentication, authorization, roles and privileges to various systems providing physical and/or logical access to end users. Often, the IDMS contains data within a centralized database that is authenticated against and/or shared with the ACS, Active Directory, Other Service Providers, Security Token Services, Digital Identities, Identity Providers, Services Providers, SAML 2.0, OAuth, and RBAC.

4.5.14 Emergency Response Systems

Protecting the systems used during emergencies is vital to business continuity during emergency incidents. While these systems may ride on the same premises distribution backbone, additional controls should be established to provide redundancy to ensure they stay up and active.

4.5.14.1 Computer Aided Dispatch

Computer aided Dispatch includes the automatic handling of events, including SMS messages, trouble-ticket logging and activation, and paging. These are typically linked to GIS information to provide location data to the responders.

4.5.14.2 e911

e911 is a provision of emergency telephone service from anywhere within the airport perimeter to a 911 operator who can then expedite the call to the appropriate agency. e911 calls can also occur from travelers' cell phones, which increases the need for a robust Distributed Antenna System facility. Depending on the specific airport, e911 calls may be responded to by airport personnel or local city or county agencies. Additionally, airports may provide "511" services within their perimeters. These are non-critical transportation-related inquiries.

4.5.14.3 Fire Suppression and Alarm Systems

Sometimes part of a Building Management System, these systems detect smoke and/or heat, and initiate an alarmed response to the command and control center. These systems include smoke- and heat-monitoring devices that trigger alarms and sounders, and audio and visual paging notifications upon smoke and/or heat detection. The system can also be configured to unlock emergency evacuation doors and to notify civil emergency authorities.

The fire-fighting or suppression system includes water sprinklers and other devices to extinguish a fire. Different suppression systems are required for different types of fires (e.g., electrical fires as opposed to wood or fabric). For IT rooms, dry-type fire-suppression systems are preferred, if allowable by local fire codes.

4.5.14.4 Emergency Response Systems

Emergency response methodologies and systems coordinate an airport's response to major incidents. These include air crashes, both on and off the airport, terrorist and criminal activity, and other incidents such as fatal wrecks or accidents involving staff, passengers, or members of the public. This system should also integrate with natural disaster responses and fires.

4.5.15 Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) has evolved since the mid-2000's as a blend of Security Information Management and Security Event Management products. This powerful combination provides a system capable of bringing together digital log files, containing various types of data, from all systems vital to airport security. A sampling of the data types below puts a SIEM into perspective from an airport operator standpoint:

- Video Surveillance Systems
    - Unauthorized access attempts to cameras
- PIDS
    - Intrusion breach attempts
- Video Analytics and Video Synopsis
- Communication Systems
    - Unauthorized access attempts
- LAN Systems
    - Workstations
        - Unauthorized access attempts
        - Physical access attempts
    - Servers
        - Unauthorized access attempts
        - Physical access attempts
        - Temperature and humidity readings
    - Firewall Data
        - Denial of service attacks
        - Website blocking
        - Port access attempts
        - Data requests
        - Computer access to systems
    - Switches and Routers
        - Data pathways taken by security systems
- Intrusion Prevention Systems
- Antivirus Servers
- Endpoint Security Suites
- Mobile Device Management
- Operating system data
    - Login attempts

Many SIEMs out of the box or off the shelf come with a default configuration for logging. Adjusting the controls for logging to include additional systems can lead to better results in data and log collection.

4.5.16 Other Resources Vital to Airport Security

In the Office of Personnel Management data breaches that were reported in 2015, hackers, once inside the network, had access to not only personnel files but also technical manuals and documents that were not password protected or encrypted. These manuals were most likely used to gain access to other areas of the network, as the hackers were able to ascertain which hardware was on the network and exploit its vulnerabilities (Committee on Oversight and Government Reform 2016).

Resources that are not directly vital to airport security, such as technical manuals and password lists kept in documents, can be a resource to obtain access to a vital airport security system. The National Safe Skies Alliance synthesis *Findings and Practices in Sharing Sensitive Information* identifies “Privileged Materials” that are not classified or designated by federal or state regulations and laws, but are deemed privileged (Safe Skies 2016). Documents may be protected under the Federal trade secret/proprietary laws, such as the Economic Espionage Act of 1996, or state laws, making them exempt from the Freedom of Information Act (FOIA) of 1967. Some documents or electronic files pertinent to this guidebook include:

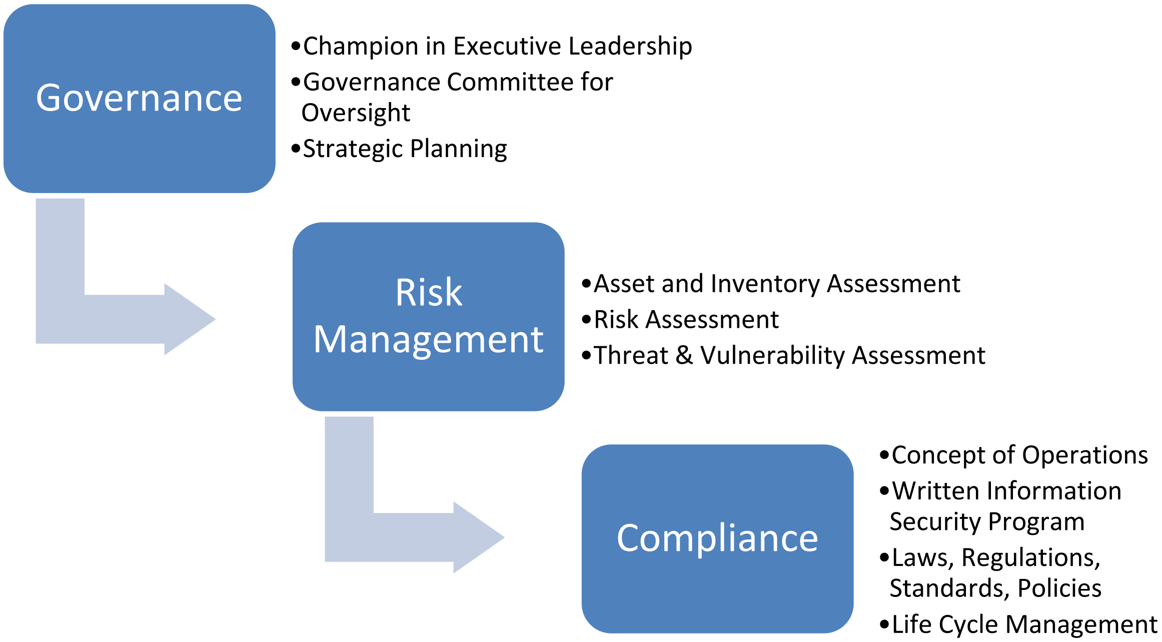
- CCTV footage
- Company/organization SOPs, and policies and procedures
- Construction drawings/layouts and video, especially showing:
    - HVAC and utilities (electrical, gas and telecommunications)
    - Hardware, such as door locks
    - IT infrastructure

SECTION 5: FINANCIAL AND OPERATIONAL CONSIDERATIONS

5.1 Introduction

The goal of this section is to bring the guidebook together into actionable items for the airport operator. At this point, an understanding of the airport environment, airport security areas, systems vital to airport security, threat types, security controls, governance, standards, and best practices has been developed through the previous sections using the GRC model shown in Figure 13.

Figure 13. Governance, Risk Assessment, Compliance


Governance
•Champion in Executive Leadership
•Governance Committee for Oversight
•Strategic Planning
Risk Management
•Asset and Inventory Assessment
•Risk Assessment
•Threat & Vulnerability Assessment
Compliance
•Concept of Operations
•Written Information Security Program
•Laws, Regulations, Standards, Policies
•Life Cycle Management

5.2 Financial Considerations

An airport operator must always use the best facts available to determine how to fund risk protection. What is the likelihood of a particular threat? What level of investment is necessary to mitigate or thwart that threat? At what point is investing in protection from a certain threat no longer cost effective? What are the competing interests, especially other risks? These questions pose very real challenges for the facility operator while balancing the moral question of “how much is enough?” with the business question of “how do we fund this?”

Financial decision making can be supported with consensus-driven rank-ordering of the threats/risks, using elicitation sessions with key stakeholders. Using subject matter experts to vet approaches to risk mitigation, response, and, in some cases, avoidance, can greatly enhance the financial decision process, and certainly assists in the ever-present cost justification exercises that need to pass muster with governing bodies responsible for approving investments.

In the final analysis, the key decisions will be supported with subjective consensus agreements that are counter-intuitive to the financial mindset. This is largely due to the difficulty of placing a dollar value on the effects of something that has not happened yet, and may never happen. Even more difficult are attempts to apply a value to the human toll of an event that may never happen. In response to Homeland Security Presidential Directive (HSPD)-16, DHS/TSA considered applying a cost of human life in a 2008 program assessing threats to the national aviation system and potential damage due to specific threats; it was ultimately abandoned because no real scientifically acceptable measure existed. So, the airport facility operator must continue to use the best information and counsel available in devising a strategic approach to financial considerations associated with mitigating security risks.

5.2.1 Grant Funding Considerations

A number of grants are available through DHS to "enhance the ability of regional authorities to prepare, prevent and respond to terrorist attacks and other disasters" (DHS 2017) through planning, equipment, training and exercise needs. *Recommended Security Guidelines for Airport Planning, Design, and Construction* (Safe Skies 2017) provides an overview of the funding mechanisms that can be used to help with projects to protect access to vital security systems through TSA Other Transaction Agreements. Other grant options can be researched online through the following resources:

- FEMA – https://www.fema.gov/grants
  Preparedness grants funding provided to state, local, territorial, and tribal governments in the form of non-disaster grants
- DHS Research Grants, Science and Technology Directorate – https://www.dhs.gov/research-business-opportunities
  Investments in scientific research leading to the development of new and innovative technologies that are transitioned to customers to enhance their mission capabilities

5.2.2 Procurement Considerations

Procurement strategy vehicles such as the Request for Proposal (RFP) and Request for Qualification (RFQ) can lead to a lengthy procurement time that is not always conducive to the critical nature of securing systems impacting airport security. Table 12 describes procurement vehicles, including pros and cons for each when considering planning and design processes impacting airport security systems.

Table 12. Procurement Vehicles Pros/Cons Table

Procurement Vehicle	Description	Pro	Con
Standard Quote	A line item request with few details	Known price	Unknown scope of services
RFQ	Only qualifications and experience are submitted for review	A comprehensive listing of subject-matter experts (SME) and their skill sets, historical knowledge, and project experience	No contract to execute for services Additional RFP or Scope of Work Needed
RFP	Solicits proposals made through a bidding process	Standard and formal process with a schedule and milestones	Typically, a lengthy process
Open RFP	Same as RFP, however any potential supplier can view documents and submit a response / bid	Many submissions, thereby allowing many solutions	May receive unqualified bids or responses

Procurement Vehicle	Description	Pro	Con
Closed RFP	Same as RFP; however, issued to specific invited respondents only	Fewer submissions, narrowed focus	May not have any proposals if list is too short and the skillsets/qualifications cannot be met
On-Call Agreements	Multiple qualified firms available to complete task orders	Quick access to SMEs Faster response	Historical knowledge lost when firm does not rebid new term or win

Both grant and procurement processes should be identified as part of the business workflow in any airport-driven initiative or project. Governance Committees and/or project managers, as a best practice, work these blocks of time into their schedules, and include collaboration and communication with the necessary stakeholders.

5.3 Operational Considerations

The overall approach an airport takes to achieve its security objectives is most often referred to as Concept of Operations or ConOps. Protecting access to systems involved in security is a part of the overall concept. The need exists for airport operators to properly define, establish, and document user requirements that determine access levels, roles and responsibilities, and response to incidents, including those involving access to vital airport security systems.

When discussing access to vital systems, administration and management should be part of an airport's ConOps. Historically, ConOps has been defined as how an airport achieves safe and secure operations during normal and emergency airport activities. In its simplest form, a ConOps provides a carefully articulated plan for developing a system capable of responding to various possible scenarios, usually identified through the threat/vulnerability assessment (TVA). Of particular importance is how the airport will respond to off-nominal events where external stakeholders must be involved, which is almost always the case. These stakeholders (internal and external to the airport) must come together in order to program and plan for response, decision making, support, and reaction to such events, establishing requirements for information, data/communications, and organizational constructs such as chain of command.

The structure of the ConOps for emergency response is usually mapped to the National Incident Management Systems (NIMS), Incident Command System (ICS) structure. As identified in the Governance Framework section, a Steering Committee is used to develop the ConOps into a form that is agreed upon by all stakeholders, and then taking the proposed ConOps through a series of validation and verification efforts to ensure the approach is sound.

According to ACRP Report 93, ConOps includes "…roles and responsibilities, individual plans for functional recovery, functional recovery prioritization, plan activation, and plan deactivation" (ACRP 2013, 30). When considering how effective a ConOps is in responding to various scenarios, the airport operator and stakeholders can challenge or vet the envisioned steps in a committee or a tabletop exercise to ensure the desired outcome.

Roles and responsibilities of staff when the airport's business continuity plan and or emergency response plan is activated includes:

- Incident Command Post (ICP) under ICS
- Emergency Operations Center
- Damage assessment team generally forming under a strike team within the ICP
- IT recovery team(s) generally forming within the ICP

While these committees or working groups have an active role in dealing with the crisis at hand, they also have an active role in recovery and the return to normal operations as quickly and effectively as possible. A major component of that is ensuring the airports' vital operating systems are protected. This protection only becomes real after appropriate planning and implementation. In order to ensure effective and efficient recovery takes place, each system and the staff that support, maintain, and operate that system need to be considered. The following are questions to consider during ConOps planning:

- What systems are critical to airport operations?
  - Make a prioritized list

For **each** system, answer the following questions:

- Who "owns" the system (is the operator or the IT department likely to provide support)?
- Who operates the system?
- Who maintains and/or supports the system?
- What are the data requirements?
- Is the data backed up?
  - If yes, when, where, and how?
  - How easily is the data accessed?
- Can the airport function without the system operating for a brief period of time?
  - How long can the system be down?
  - What can NOT be accomplished without the system operating?
  - Is there an effective failover plan and has it been exercised?
- What are the access requirements for the system?
  - Can it be accessed via a web portal?
  - Does the system need to be accessed via a LAN or Security LAN?
  - For non-airport users, is there an MOU (Airport Operations) and Third-Party User Access Policy (Airport IT) in place for access to view-only and/or shared data (e.g., shared video files)?

Once these questions are answered for each system, a plan can be built around operating and supporting those systems that are critical to airport operation during events and the recovery that follows.

5.3.1.1 Logical Starting Point

The organizational chart of the airport and the functional assignments of staff are good starting points for developing a ConOps for security maintenance operations. While certain stakeholders have an obvious security mandate (e.g., airport law enforcement and TSA), others operate under similar mandates (e.g., airport operations and air carrier operations). Establishing the routine operations and maintenance of the airport's system-of-systems security operation is paramount to any response protocol associated with an off-nominal event (such as an attempted breach). This approach must consider the system life cycle in terms of operations, maintenance, problem response, and change management when regulations shift, or regulatory mandates adjust.

One critical aspect of ConOps development, particularly as it relates to emergency response and recovery, is that it must reflect the standing relationships between individuals and departments alike. Ensuring the chain of command remains consistent will vastly improve the acceptance and understanding by all persons involved.

5.3.1.2 Organizational Response

The second driving element of a ConOps is how the organization responds to an unexpected event; anticipated and agreed-upon roles and responsibilities and acceptable standards of response are critical. Generally, the NIMS is a solid starting point for emergency and/or disaster planning. Within this model is the ICS model that is generally accepted by all emergency responders. The strength of the ICS model is its loosely structured approach that incorporates a variety of organizations involved. It is flexible enough to mold to the specific circumstances, but structured enough to align to best practices of emergency responders within the NIMS model.

Response planning, as a best practice, should involve the NIMS model. It is critical to consider and account for those local processes and procedures that are required for intergovernmental coordination and local nuances of the airport's owner and operator. NIMS serves as a structure for emergency response; it necessarily considers business practices and relationships within the airport's operating structure, as well as the airport owner and operator's relationship with those outside agencies that will respond during emergency events. Understanding and making note of these relationships is critical to disaster response ConOps planning and success.

All adjacent stakeholders must be involved in planning, exercises, and communication priorities. This becomes even more critical when command naturally passes from one agency to another as the response matures. For example, once an aircraft fire is out and all injured have been recovered, command at the incident command post passes from an ARFF lead to an Operations lead in order to begin recovery procedures and return the airport to full operations (within the confines of NTSB coordination, of course). Command relationships are an important factor in ConOps development, as further discussed below.

5.3.1.3 Organizational Relationships

The third element to ConOps planning is that of understanding the relationships between individuals and departments at the airport and the mutual aid agencies who respond to airport emergencies. At some airports, a local airport authority has been established and that organization employs both police and fire units at the airport. At other airports, some police duties are handled by the local city or county that owns the airport; and still others have ARFF services provided by the local city or county units as well. Each airport is different and understanding the reporting relationships is critical to understanding the level of detail necessary for ConOps development. While these relationships typically have been woven into the day-to-day operations, it is important for them to be part of the emergency response planning as well.

Cities and/or counties might be the single provider of the IT systems utilized by police and ARFF personnel. Airport governance plays a role in the initial planning (e.g., independent or quasi-public authorities usually own/operate all their systems, while city or state-owned airports often depend on organizations outside the airport footprint).

5.3.2 Testing and Quality Assurance of Physical Systems

Once a ConOps is established, the airport operator will have a blueprint that gives a high-level overview of department collaborations, roles and responsibilities, systems used and awareness of access types (e.g., remote access users, data room access, and physical plant/room locations). An airport operator can use the ConOps as a guideline reference during the testing/quality assurance phase of a project, particularly to understand the access types involved within a particular system.

During installation and implementation of physical and logical systems, the integrator is often tasked with providing proof that the systems perform to the specification outlined by the airport operator. Once performance and acceptance testing (e.g., commissioning) is complete and verified (often through an independent third-party SME hired by the airport), airport security and IT will want to document the acceptance and processes by which each system was tested.

> *"If properly conducted, testing and maintenance activities can minimize equipment failures, forecast impending operational problems, identify functional weaknesses, and guide future upgrades and improvements." (Physical Security Systems Assessment Guide, U.S. Department of Energy)*

With most vital systems located in telecommunication rooms or data centers, best practices in testing and quality assurance can be found in the ANSI/BICSI 002-2014 for data center design. Table 13 provides a few examples.

Table 13. Example Quality Assessment Tests for Physical Security Assets

Example Protection Mechanism	Example Testing / Quality Assurance
Bullet-Resistant Glass or Glazing If the threat of gunfire or other projectiles is present, the data center should consider the use of bullet-resistant glass. During evaluation, the nature and type of attack being protected against should be noted in the risk analysis portion of the GRC model. Security designers for example can use the BISCI standards referencing UL 752, which quantifies resistivity based upon the ammunition used and shot patter or placement.	• Level 1 – 4.8 mm (3/16-in) thick, solid, open-hearth steel with a tensile strength of 345000 kPa (50,000 psi) or 9-mm full copper jacket with lead core, 124 grain at 358 m/s (1,175 ft/s) –3 shots • Level 2 – 0.357 Magnum lead soft point, 158 grain at 381 m/s (1,250 ft/s) – 3 shots • Level 3 – 0.44 Magnum lead, semi wadcutter gas checked, 240 grain at 411 m/s (1,350 ft/s) – 3 shots • Level 4 – 0.30 caliber rifle lead core soft point, 180 grain at 774 m/s (2,540 ft/s) – 1 shot
Break-Resistant Glass or Glazing A window or door containing glass that is in a high-risk area should be evaluated for its resistance to break-in.	• Single blow impact testing (smash and grab) • Multiple impact testing • High-energy impact testing • Performance
Physical Fences and Metal Barriers In the case of fences and metal barriers, security designers should consider that even a 2.4 m (8-ft) tall fence with three strands of barbed wire could be compromised in less than 10 seconds (ANSI/BISCI 002, 2014).	• Delay testing • Clear Zone of at least 6 m (20 ft) on both sides of the fence to prevent climbing

The airport operator can further develop these testing and quality assurance efforts by using the forms listed below and integrating them with their Written Information Security Plan (WISP) “Operational Controls, Certification, Accreditation & Security Assessment” section as outlined in Appendix C of this guidebook.

- Operational Controls
    - Certification, Accreditation & Security Assessment
    - Contingency Planning
    - Incident Response
    - Maintenance
    - Media Protection
    - Physical & Environmental Protection

Prebuilt forms and checklists can be found in the U.S. Department of Energy (DOE) Physical Security Systems Assessment Guide (DOE, 2016):

- Appendix A: Intrusion Detection System Performance Tests
- Appendix B: Access Control System Performance Tests
- Appendix C: Communication Equipment Performance Tests
- Appendix D: Support System Performance Tests
- Appendix E: Personnel and Procedure Performance Tests

5.3.3 Operation and Maintenance of Physical Security Systems

The longest duration in the life cycle of a physical security systems is the operation and maintenance (O&M) phase. During this phase, the systems should be properly maintained in a secure manner, consistent with the program controls developed by the airport (e.g., using the Security Controls and Countermeasures Matrix found in Appendix B). Additionally, airport staff applying proper accountability and oversight of these systems can establish operational efficiency and effectiveness through the adherence to policies and requirements that were established during the governance process.

The following functions and processes are necessary to ensure that physical security systems are managed in a manner that promotes their adherence to the CIA Triad.

ASSET MAINTENANCE

Every component in a physical security system needs an appropriate schedule that addresses periodic maintenance reviews, patching and version upgrades where applicable, periodic testing to ensure the system is operable, and component replacement. The maintenance schedule must comply with vendor recommended practices, and reviews should be conducted strictly within the prescribed timeframes. Each maintenance review must also be documented with any findings regarding component condition.

Best Practices for Asset/Inventory Management:

- *Use of asset database software to manage assets*
- *Integration with IT Helpdesk for Incident Management*
- *Integration with Financial System for Asset Lifecycle Replacement Planning*
- *Integration with Compliance Software for monitoring technical compliance*

PATCHING AND VERSION UPGRADES

Hardware components likely will need patches or upgrades to their associated software periodically. A patch is typically issued when the software vendor finds a flaw in the existing software version and feels that there is a need to address it immediately. This often occurs when the flaw or bug is security related. Software may also be occasionally updated to a new version when the vendor has batched a number of changes, sometimes with new features and functionality.

In either case, the software patch or new version should be assessed in a test environment, often referred to as a “sandbox,” to ensure that the new version or patch will work correctly in the airport’s existing environment. Thorough testing is essential to ensure that an unexpected error does not arise due to the change.

ASSET INVENTORY

Every physical security system needs a comprehensive list of its hardware, software, middleware, utility program, and firmware components. The list needs to be continually updated with a thorough description of each component, including part number or software license number, estimated value, replacement date, and, where applicable, a periodic maintenance schedule.

There are two very important reasons for maintaining a detailed asset inventory. First, the airport finance department is likely depreciating the value of the assets for accounting purposes. Second, all systems eventually need to be replaced.

SYSTEM CONFIGURATION AND ARCHITECTURE

All systems change over time, and physical security systems are likely to experience more changes than most, as the security posture of an airport is continually in flux. Every change to the system must be considered through a configuration change management process. No changes should be made to a physical security system without all necessary stakeholders being informed of the potential change and given an opportunity to provide comments.

A change management board is often established as an oversight group, and change management software is typically employed to announce proposed changes, gather comments, and document the final decision. If an airport has an existing change process for other airport technology systems, then it should be expanded to cover all physical security systems. If an airport does not have an existing system, one must be established. Configuration management is a critical system maintenance function, and its importance cannot be over-emphasized.

An important component of configuration management is to maintain an asset valuation of the total physical security system. Systems have a tendency to grow if appropriate controls are not in place. For example, a PACS is likely to have doors added after the initial implementation. Every time a door is added, there is a growing cost for the O&M of the entire system. Additional costs to software licenses, capacity on hardware, and contractor maintenance can all be impacted by system growth.

ROUTINE TESTING

Every physical security system must be periodically tested to ensure that it is fully operational. There is often a misconception that systems that are used daily do not need testing. However, a system may use some of its functionality on a routine basis, but other functions are only used in emergency situations. When an actual emergency does occur, those functions may not be ready for use, and the airport may face a system failure at a critical time.

All functions on a system should be tested at least semi-annually. However, there are some systems that should be tested daily. For example, duress buttons and ring-down phones must be tested daily to ensure that they are operable. The test not only exercises the system components, but also ensures that the personnel charged with operating and using the system are fully acquainted with all aspects of its use.

PERFORMANCE MEASUREMENT

If the airport established KPIs and metrics for its physical security system during the acquisition phase, regular monitoring and auditing of the system is necessary to ensure that the system is performing according to the desired expectations. Performance measurement can be conducted in conjunction with routine system testing or may be conducted on a less frequent basis, but no less than once a year.

ONGOING PERSONNEL TRAINING

Though a physical security system may be in place for many years, it is highly likely that the personnel operating the system will change over time. When a system is first acquired, extensive training is provided to all users. However, refresher trainer for existing personnel or orientation for new personnel is often overlooked. Training should be conducted once every six months for all staff members that are using the system. When new staff members come aboard, a system orientation must be conducted to ensure proper usage.

An important component on the training is establishing a clear link between the training curriculum and the mission/goals of the system, with a thorough explanation of the importance of the system in the overall security posture of the airport.

SYSTEM DOCUMENTATION

Over time, the documentation that was originally delivered with a system will evolve as the system is upgraded, modified, and/or expanded. All system documentation must be routinely reviewed to ensure that it reflects the current system environment.

DISPOSAL OF PHYSICAL SECURITY SYSTEM COMPONENTS

All systems are upgraded over time and components are periodically decommissioned. The airport must be cognizant that any component with embedded memory must be disposed of in a manner that ensures that it retains no confidential information. If the airport employs a third party to dispose of such components, it must regularly check to ensure that the destruction is being properly carried out. The following steps should be considered:

- **Place equipment in a secure area for temporary storage before it is recycled:** This “holding area” should not be a public place such as a hallway or loading dock.
- **Arrange for proper disposal of equipment:** As discussed above, this could be by a third party or, if done internally, should be using proven destruction methods. Equipment can be destroyed physically, by puncturing, shredding, heating, vaporizing, or some other method that permanently eliminates any use of the equipment.
- If the physical security system is managed by an airport entity other than the airport IT department, a consultation between the two groups will likely identify shared resources to accomplish the task.

5.4 Governance in Action

The Governance Framework was discussed at length in Section 3. Ensuring a clear vision of the airport’s strategy and goals for technology and physical spaces goes beyond protecting access. However, the scope of this guidebook is focused on governance in reference to access. The key imperatives of governance, best practices found in the field and in industry standards, and their associated governance sections are shown in Table 14.

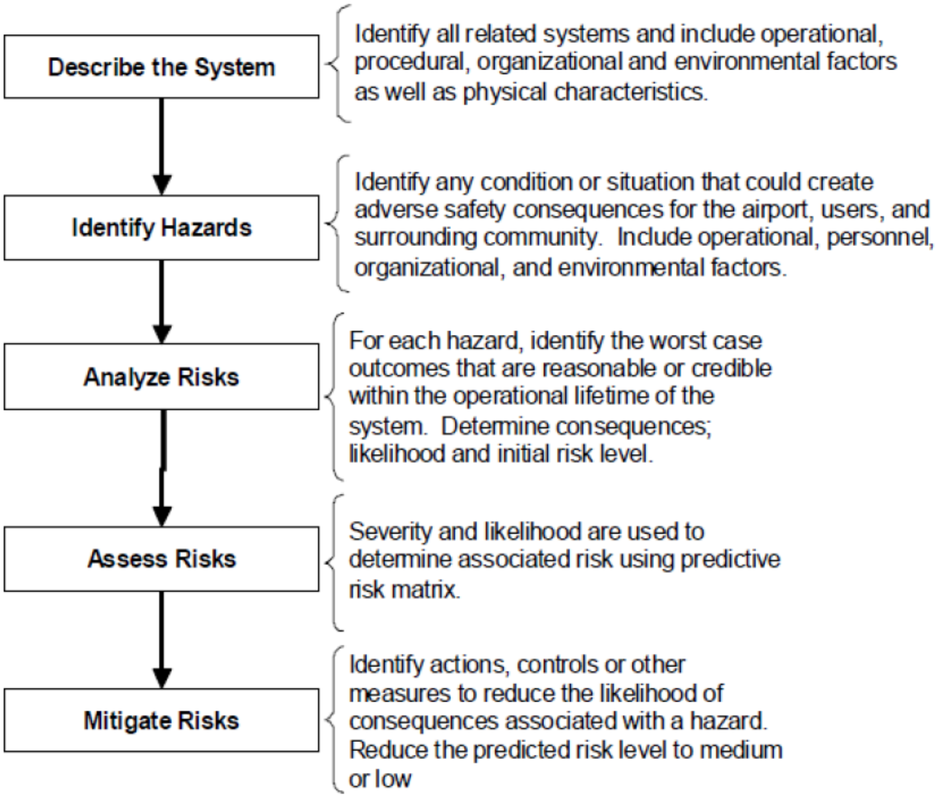
Table 14. Key Imperatives and Best Practices Table

Key Imperatives	Best Practices	GRC Toolkit
Sanctioned by Airport Director	Outline as a Strategic Goal or Initiative in the Airport’s Annual Strategic Plan	Governance Section: Charter
Purpose of Governance Committee defined	Define and formally constitute committees to be used for governance oversight. Decide early on, which departments will be included (e.g., Operations, Safety/Security, IT, Public Relations, etc.)	Governance Section: Example Functional and Project Org Charts
Clearly stated roles and responsibilities defined	Governance Committees at a minimum should include one technical and one business. Each carries out responsibilities of decision-making powers Sets formal meeting times and agendas	Governance Section: Roles and Responsibilities
Adherence to strategic initiatives of the airport	Reference to mission and vision statements, including strategic goals when creating the Governance Charter and defining roles and responsibilities	Governance Section: Governance Charter Roles and Responsibilities
Guidelines are clear	Airport Director and Key Staff establish a list of guidelines to be followed as part of governance	Governance Section: All
Accountability and Success measurements	Using global KPIs already established in the organization to measure accountability and success	Governance Section: All
Managing Access Levels for VMS	Use of an MOU	Governance Section: All

5.5 Risk Management in Action

Risk management is the fundamental process of proactively managing risks before changes to the system are made. When sensitive systems are changed or modified, or changes are made regarding who has access to those systems, a risk management process should be used to ensure any new threats or hazardous conditions are identified and mitigated to an acceptable level of risk. The typical and accepted risk management process is five steps, as shown in Figure 14.

Figure 14. Risk Management Processes


Describe the System
Identify all related systems and include operational, procedural, organizational and environmental factors as well as physical characteristics.
Identify Hazards
Identify any condition or situation that could create adverse safety consequences for the airport, users, and surrounding community. Include operational, personnel, organizational, and environmental factors.
Analyze Risks
For each hazard, identify the worst case outcomes that are reasonable or credible within the operational lifetime of the system. Determine consequences; likelihood and initial risk level.
Assess Risks
Severity and likelihood are used to determine associated risk using predictive risk matrix.
Mitigate Risks
Identify actions, controls or other measures to reduce the likelihood of consequences associated with a hazard. Reduce the predicted risk level to medium or low

Source: FAA Office of Airports Safety Management 2012

The application of risk management is critical to ensuring that risks are managed proactively. Managing risk reactively can be expensive and increases exposure to threats. Therefore, when changes are proposed, a small group of empowered and knowledgeable SMEs should meet to walk through the risk management process. The triggers for such a group meeting include, but are not limited to:

- **A new system is brought online:** Any system with critical operational, security, or financial impacts
- **System integration where it did not previously exist:** System integration represents one of the most critical types of risks and threats to an organization's systems, because it allows more and sometimes disparate individuals access to multiple systems.
- **A proposed change in roles and responsibilities:** Organizations often reorganize with little or no thought given to how it will impact access to systems.
- **A major upgrade is planned for an existing system:** System upgrades should be discussed in the context of whether the planned changes will impact processes and procedures in any way; the upgrade should then be vetted through the risk management process.

By introducing risk management and training all those involved with securing systems in the risk management process, an organization can reduce exposure to risk and threats and focus on better management of system performance.

5.5.1 Security of Operations

Security operations decision makers should consider the findings of a thorough threat/vulnerability assessment (TVA), and at least a preliminary design effort, to address the risk posed by each threat with an appropriate measure. These measures may simply be avoidance of a risk, or may encompass a focused defeat-driven set of measures. Regardless of the details on how an airport approaches its security measures, the airport operations should undergo a process whereby the measures and systems envisioned are evaluated through managing assets and inventory, TVA, and countermeasures. This process can be completed through the CRAMM methodology, and is described in the Risk Management section of Appendix A: Governance, Risk Management, and Compliance.

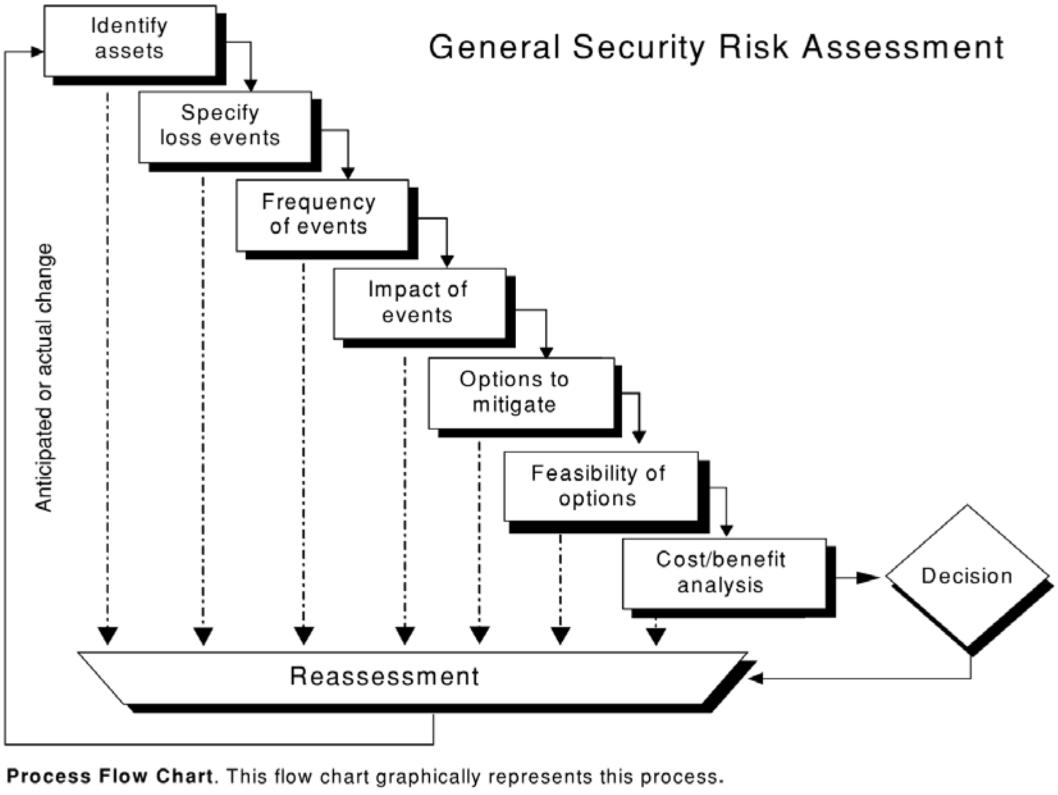
5.5.2 Threat and Vulnerability Assessment (TVA)

Vulnerability assessments are designed to yield a ranked or prioritized list of a system's vulnerabilities to various kinds of threats. Organizations that use these assessments are aware of security risks and understand they need help identifying and prioritizing potential issues. By understanding their vulnerabilities, an organization can formulate solutions and patches for incorporation with their risk management system.

The perspective of a vulnerability may differ depending on the system assessed. For example, a utility system, like power and water, may prioritize vulnerabilities to events that could disrupt services or damage facilities, like calamities, tampering, and terrorist attacks. An information system, like a website with databases, may require an assessment of its vulnerability to hackers and other forms of cyberattack. On the other hand, a data center may require an assessment of both physical and virtual vulnerabilities because it requires security for its physical facility and cyber presence.

In Figure 15, the ASIS International Guideline includes a seven-step process that can be used to identify security risks at a specific location, and focuses on reassessment after each step.

Figure 15. General Security Risk Assessment



Process Flow Chart. This flow chart graphically represents this process.

Source: ASIS International 2003

5.5.3 Countermeasures

A listing of countermeasures, organized by functional security controls is outlined in Appendix B: Security Controls Matrix.

Using good risk management techniques prepares the airport operator for unknown events. The Risk Management checklist below gives the airport operator a good starting point for launching a successful Risk Management program.

- ☐ Identify resource (e.g., Subject Matter Expert Consultant, Staff) to manage the creation and maintenance of the WISP
- ☐ All governance checklist items completed
- ☐ Identify all physical locations and logical systems vital to airport security (see Section 4: Security Controls and Vital Systems)
- ☐ Perform Asset/Inventory Assessment
- ☐ Perform Threat and Vulnerability Assessment

5.6 Compliance in Action

Outlining the laws, regulations, standards, and policies needed to guide the ongoing protection of the systems impacting airport security is the first step in the administration of compliance. A Written Information Security Program (WISP) provides definitive information on the prescribed measures used to establish and enforce an information and physical security framework.

5.6.1 Integration with the Airport Security Program/Plan (ASP)

The Airport Security Program, as part of CFR § 1542, outlines the specific requirements set forth by the TSA for developing a viable airport security program through an Airport Security Plan (ASP). TSA also provides guidance and direction through Security Directives (SD) and Information Circulars; compliance with SDs is mandatory. The ASP must also address contingency operations and incident management. These plans are considered protected under federal law from disclosure outside those entities required to operate under their mandate.

> *Although it is not required to integrate references to access types, levels, controls, or policies into the ASP, it can be a good practice in supporting protection of systems and physical spaces that are vital to airport security.*

In general, the ASP is made available to airline tenants as an SSI-marked annex to the airport's certification manual. These documents outline the routine and contingent operational footprint for security at an airport, and encompass much of the detail discussed above.

Table 15 provides the ASP sections where references to types or levels of access to systems occur.

Table 15. Airport Security Plan Reference Table

Section	Description	Reference to Access Types and Levels or Policies
I. Disclosure Statement / Security Responsibilities	Distribution of these Security Procedures should be restricted to individuals with a legitimate need for access to them. Identify the individual who has the responsibility for the development, upkeep, and administration of the Airport Security Procedures	ASP should reference the groups and/or individuals with direct access to the ASP
II. General Information	Forward Introduction and Purpose Distribution Name and Location of Airport Airport Activities Airport Description Emergency Phone Numbers	ASP should list in Distribution who will receive a copy of the ASP
III. Definitions and Terms	Definitions and Terms	Terms associated with physical and technological access (such as Third-Party User Access Policy) should be defined
IV. Administration	Airport Operator Individual Responsible for Airport Security	Maintain a complete and current list of all individuals with airport access
V. Aircraft Movement Area / Security Control	Aircraft Movement Area Perimeter Controls	Perimeter Controls – Describe any perimeter barriers or access controls (such as fencing, gates, access control systems, airport locks, key control systems)
VI. Airport Security Procedures	Aircraft security requirements Ped/Vehicle access Challenge procedures Reporting of suspicious behavior	Should describe the procedures revolving around requirements for access, challenge procedures, and reporting of suspicious behavior
VII. Airport Emergency Grid Map	Emergency Locator Map for: Emergency Response Personnel Law Enforcement Airport Personnel	Access areas should be well highlighted to show specific levels of access to secured areas

Section	Description	Reference to Access Types and Levels or Policies
VIII. Identification of Airport Personnel	Methods/Systems and Procedures for ID Badge/Card Application Procedures Acceptable forms of ID Temporary Airport ID Uniforms with identifiable markings	Identity Management systems can be used to help maintain this information and referenced as such in the ASP
IX. Identification of Vehicles	Methods/Systems and Procedures for Authorized Vehicles Special Paint/Markings Decal in Specific Location Hang Tags	Identity Management systems can be used to help maintain this information and referenced as such in the ASP
X. Law Enforcement	Describe agreements and responsibilities between airport and Law Enforcement agencies to provide support Communication Types and Procedures	Specialized access or escorted access to secured areas should be referenced via an MOU or Mutual Aid Agreements
XI. Special Events	Procedures for Special Events Air Shows VIP Visits Events with unusual numbers of people at airport	Access areas should be well highlighted to show specific levels of access to secured areas Identity Management systems can be used to help maintain this information and referenced as such in the ASP Reference Access Levels associated with emergency incidents
XII. Increased Security Threats	Procedures how security is implemented during Homeland Security Advisory System levels	Reference Access Levels associated with emergency incidents Include reference for cyber security through DHS's Cyber Information Sharing and Collaboration Program (CISCP)
XIII. Aviation Security Contingency Plans	Contingency plans and procedures for incidents such as: Bomb Threats Civil Disturbances Crowd Control Air Piracy Suspicious Items	Reference elevated access levels for contingency plans. Reference internal policies and procedures (such as the Business Continuity Plan, Disaster Recovery Plan, and the Acceptable Use Policy through Information technology)

5.6.2 Written Information Security Program (WISP)

A holistic approach to information security involves the creation of the WISP. This approach can be written to either ISO 27001/27002 or NIST 800-53 standards, depending upon the organization's preference. A WISP documents the measures that the organization takes to protect the security, confidentiality, integrity, and availability of both information (data) and physical security. A sample WISP outline is presented in Appendix C and can be modified/tailored to the airport's needs (e.g., not all sections of the WISP need to be filled out, if not applicable).

A WISP document is beneficial because it provides a way for the airport operator to keep and maintain all compliance requirements and best practices in one place. For example, Practical Law defines the WISP's objective as:

> "…defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards [COMPANY] has selected to protect the personal information it collects, creates, uses, and maintains. This WISP has been developed in accordance with the requirements of the Massachusetts Data Security Regulation, Mass. Regs. Code tit. 201, §§ 17.01-17.05, other similar US state laws, and [LIST ADDITIONAL APPLICABLE LAWS AND OBLIGATIONS]" (Practical Law, 2017)

The following WISP checklist gives the airport operator a starting point for launching a successful program:

- ☐ Staff has been identified to manage the creation and maintenance of the WISP
- ☐ All Governance checklist items have been completed
- ☐ All Risk Management checklists have been completed
- ☐ ASP has been aligned with WISP (see Table 15)
- ☐ WISP document created using template in Appendix C

5.7 Preparing Systems and Networks for Planning, Design, Procurement, Implementation, Monitoring, and Controlling

A perfect time to apply governance, risk management, and compliance (GRC) is during airport construction or renovation projects. Adherence to the steps with GRC ensures that the project creates the best possible solution for the security of systems and spaces.

In addition to the airport's design document guidelines and ASP, the documents created as a result of following the GRC toolkit in Appendix A will provide critical information to planning and design consultants, vendors, and contractors during procurement and implementation. Once implemented, airport staff members will be tasked to monitor and control systems and spaces.

Many technologies are never mentioned or referenced in an airport's design document, partly due to the rapid evolution of technology advancements. However, foundational technologies exist and can be included in the design documents, depending upon the maturity and skillsets of the airport's IT department and/or outsourced IT resources. A quick reference of these technologies and an example of each is included below:

Campus Fabric Design – A fabric is an overlay, which is a logical topology used to virtually connect devices on top of an arbitrary underlay technology.

Ex. *Cisco's Design Zone for Enterprise Networks* is a workspace for IT professionals to gain experience in enterprise areas such as campus fabric design, campus wired and 802.11 wireless network design, WAN/branch and internet edge design, and mobility design.
Source: http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-borderless-networks/index.html

Another campus fabric design uses interrelated building blocks for network management and orchestration, focusing on data traffic that is bandwidth-intensive (e.g., HD video) and delay-sensitive (e.g., mobility).

Ex. HP FlexNetwork Architecture is a framework workspace for IT professionals to gain experience in enterprise areas such as mobility, virtualization, high-definition video, rich-media collaboration tools, and cloud computing security. Its focus is on application-driven, service-oriented architectures and virtualization in conjunction with on-premises security solutions.
Source:
http://www.hp.com/hpinfo/newsroom/press_kits/2011/InteropNY2011/FCRA_Architecture_Guide.pdf

Secure Network and Cloud Controls – Software controls large pools of computers, storage, and networking resources throughout a data center, managed through a dashboard.

Ex. *OpenStack Networking Architecture* is a workspace for IT professionals to gain experience in enterprise areas such as deploying a secure network via the cloud, and using specific security controls.
Source: http://docs.openstack.org/security-guide/networking/architecture.html

5.7.1 Physical Design Considerations

When planning for facility protection, including general security areas and boundaries where systems impacting airport security may reside, guidance can be found in *Recommended Security Guidelines for Airport Planning, Design and Construction* (Safe Skies 2017). In concurrence with this document, the use of a ConOps, as outlined previously in this section, is highly recommended to ensure that high-level goals of an airport security system are documented and used as the initial guidelines for planning and design purposes.

SECTION 6: FUTURE RESEARCH AND CONCLUSION

6.1 Introduction

Technology is constantly advancing, so it is important to understand how this may figure into the equation when updating or upgrading airport systems. For example, the following improvements have been made to biometric access control technologies over the last decade:

- Increased matching accuracy
- Reader devices are smaller
- Exception situations have been greatly reduced
- More commercially available
- Can function under extreme weather environment
- Greater adoption from PACS vendors
- Deployment by US Government and international transportation agencies
- Non-contact fingerprint recognition now available
- NIST standards study show significant improvement in facial recognition

Other technology advances combine the ingenuity and developments in many fields such as robotics, complex logical automation, and sonar and radar.

6.2 Unmanned Vehicles

Recently, the concept of having autonomous vehicles roam around airport perimeters and within the AOA was not widely accepted. However, this concept is quickly becoming a reality. When this occurs, protecting the systems that operate the unmanned vehicles (UV) will be just as critical as protecting the financial system from cyberattack.

UVs come in many shapes and sizes. They can fly (unmanned aerial vehicle), roll across the ground, and even cross water. Incorporating UV into the daily operations at airports has and is the topic of research projects both within ACRP and PARAS. The need to understand the outside threats that are posed to such UVs is important, and protecting their operations and communications is even more critical.

The basic approach to protecting a UV operation is through encryption. Encrypting and changing codes often can slow would-be UV hackers; other protection scenarios should also be considered. However, eventually the UV may be hacked; therefore, it is imperative to plan for those scenarios.

It is necessary to provide a safe place for the airport UV in the case of loss of communications. Planning for emergency procedures should the UV go rogue is equally as important. Procedures might include the automatic shutdown of the system to render it useless to the hackers. Planning for use of UVs, and eventually problems associated with their operations, should be vetted through the risk management process, as discussed in Section 5.5.

6.3 Resilient and Intelligent Wide Area Networks (WAN)

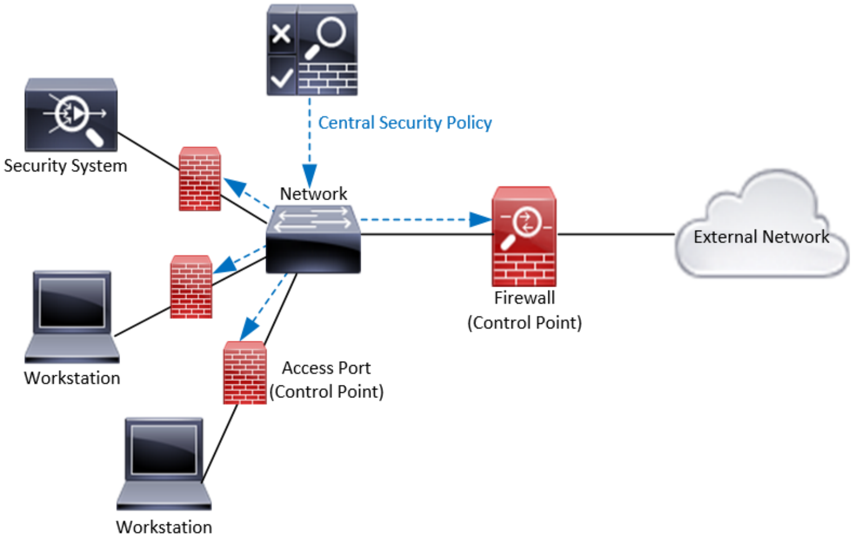
Protecting access to a wide area network (WAN) is critical. Having good network resiliency could mean the difference between the physical network being down for seconds versus hours. When designing an intelligent and resilient WAN, the solution should meet all of the items on the following checklist (as provided by resilientiq.com):

- Provide reliable and secure wireless access
- Reduce network latency and accelerate data flow
- Expedite employee production levels by allowing them to use wired and wireless solutions
- Assess bandwidth management as a best practice
- Use tools to gain network visibility, accelerate applications and reduce network traffic
- Implement smart policies
- Provide visibility into the WAN
- Reduce or limit the priority of recreational application bandwidth
- Reserve or give high priority to VoIP and thin client applications
- Allow easy appliance management, improved response time, better network control
- Help you control and prioritize the way your networks are used
- Define the maximum amount of bandwidth any particular internet site, cloud application, or user can consume
- Maintain a reliable, predictable user experience for strategic applications wherever they are used
- Identify network misuse and set sophisticated policies that restrict access to prohibited and discouraged content

6.4 Defense-in-Depth using Zero-Trust, Zero-Day Protection, and Comprehensive Security and Data Protection Platforms

While guidance for network security is readily available (e.g., Zero-Trust Network methodologies as shown in Figure 16), airports may lack the skillsets, knowledge, or staff to deal with the daily management requirements to maintain a properly secured environment involving complex software and physical mechanical components.

Figure 16. Zero-Trust Network Example for Active/Passive Network



Hacking, covert attacks, denial of service, Advanced Persistent Threats, virus or malware implantation (via an insider threat), sabotage, phishing, social engineering, and other nefarious activity could impact physical and logical access to vital systems affecting airport security. Furthermore, threats to security systems go well beyond intentional acts. The availability and integrity of security systems can also be impacted by natural occurrences and disasters, human error, as well as management neglect.

A defense-in-depth concept combines the use of multiple technologies to protect access to systems, including cloud and bring-your-own-device technologies. An example can be to use zero-trust networking with zero-day threat protection on workstations, servers, and mobile devices offering close to real-time protection, detection, and remediation.

A comprehensive security platform can protect security systems that reside on the same network as other systems and applications using these concepts.

6.5 Conclusion

This Guidebook was developed to provide airport operators with basic information required to secure technology systems that provide security for the airport, the campus, and all the people that work, visit, and use the airport on a daily basis. Airport operators need to remember that technology systems need both cyber protection and physical protection, and that the physical protection must be specifically designed for the protection of technology. Common physical protection strategies are insufficient for systems that reside in data centers, telecommunication rooms, and spread throughout the airport campus.

With a solid understanding of the landscape, locations where systems reside, and how they are vital to airport security, the airport operator can work towards creating a baseline strategy using governance, risk management, and compliance to ensure continued security of the confidentiality, integrity, and availability of systems. Armed with a working knowledge of security controls, the airport operator can then ensure that the right people and/or resources are applied to each system’s administrative, physical, and technical control types.

Securing security systems begins with a governance and management approach. Once a direction is determined and airport management is fully invested in pursuing that direction, the airport can apply the security mitigation/countermeasures required to sustain operational uptime.

This guidebook addressed the definition of airport security and covered the administrative, technological, and physical controls needed to maintain adequate day-to-day management and administrative operations.

This guidebook also laid out a plan for administering and managing various types of access to vital systems, such as video surveillance, gate and secure area access, and the physical spaces where these systems reside. It also conveyed the administrative (e.g., policies and standards), technical/logical (e.g., data and network), and physical (e.g., gates, locks, fences) security control considerations. Also covered was how to identify, assess, and prioritize methodologies, as well as create a governance framework that encompasses all risk management and compliance areas, so that systems are identified properly and adequate care is applied consistently.

As the airport establishes its security systems protection efforts, remember to utilize this guidebook as a reference and the tools and templates found in the appendices to help start the process of establishing the airport’s Governance Framework.

REFERENCES

Airport Cooperative Research Program. 2013. *ACRP Report 93: Operational and Business Continuity Planning for Prolonged Airport Disruptions*. http://nap.edu/22531

ASIS International. 2003. General Security Risk Assessment Guideline.

AT&T Intellectual Property. 2017. Centrex. https://www.att.com/gen/general?pid=9613

Aviation Security. 2016. Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates. General Accounting Office.

Berrick, Cathleen A. 2011. *Homeland Security: DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity*. GAO-10-106. Washington, DC: U.S Government Accountability Office.

Carolina. 2015. "Anonymous Shut Down Japanese Airport websites against Dolphin Slaughter." https://www.hackread.com/op-killingbay-anonymous-attacks-japanese-airports/.

CRAMM. 2017. https://en.wikipedia.org/wiki/CRAMM

Committee on Oversight and Government Reform. 2016. U.S. House of Representatives. *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation.*

Department of Homeland Security. 2017. Find and Apply for Grants. https://www.dhs.gov/how-do-i/find-and-apply-grants

Dorstewitz, Michael. 2013. "Majority of airport security breaches committed by airport employees." http://www.bizpacreview.com/2013/05/02/majority-of-airport-security-breaches-committed-by-airport-employees-66057.

FAA. 2010. 49 CFR Part 1542 – Airport Security.

FAA Office of Airports Safety Management System (SMS) Desk Reference Version 1.0. 2012.

Governance Committee Charter. 2012. Project Management Institute. https://www.pmi.org/-/media/pmi/documents/public/pdf/governance/governance-committee.pdf?la=en

Homeland Security Act of 2002. 2002. H.R. 5005, 107th Cong.

Identity Management and Credentialing Example. 2017. AlertEnterprise! https://www.alertenterprise.com

Intrusions Affecting Multiple Victims Across Multiple Sectors Report. 2017. Department of Homeland Security & the National Cybersecurity and Communications Integration Center.

Juniper Networks. 2016. Learn About Intrusion Detection and Prevention: First Edition. http://www.juniper.net/documentation/en_US/learn-about/LA_IntrusionDetectionandPrevention.pdf

Marquis, Hank. 10 Steps to Do It Yourself CRAMM. 2008. DITY Weekly Newsletter, ItSM Solutions, LLC. http://www.itsmsolutions.com/newsletters/DITYvol4iss50.htm

National Institute of Standards and Technology. 2016. DRAFT NIST Special Publication 800-63B: Digital Authentication Guideline. https://pages.nist.gov/800-63-3/sp800-63b.html

NERC CIP-006-6: Physical Security of BES (Bulk Electrical System) Cyber Systems, 2014.

Official (ISC)^2 Guide to the CISSP CBK 2nd Edition. 2010. CRC Press, Taylor & Francis Group, London.

Physical Security Systems Assessment Guide. 2016. U.S. Department of Energy. https://energy.gov/sites/prod/files/2017/02/f34/PhysicalSecuritySystemsAssessmentGuide_Dec2016.pdf

National Safe Skies Alliance. 2016. *PARAS 0008: Findings and Practices in Sharing Sensitive Information*. https://www.sskies.org/images/uploads/subpage/PARAS_0008.SharingSensitiveInfo.FinalReport.pdf

———. 2017. *PARAS 0004: Recommended Security Guidelines for Airport Planning, Design, and Construction*. https://www.sskies.org/images/uploads/subpage/PARAS_0004.Recommended_Security_Guidelines.FinalReport.v2.pdf

Resilient. Local/Wide Area Networks (LAN/WAN). http://www.resilientiq.com/localwide-area-networks.

Security Controls, Version 1.2. https://www.sans.edu/cyber-research/security-laboratory/article/security-controls. SANS Technology Institute.

The Essential Guide to Securing Remote Access. 2016. Duo Security.

Written Information Security Program (WISP). 2017a. Compliance Forge. https://www.complianceforge.com/example-written-information-security-program-wisp/

———. 2017b. Practical Law Intellectual Property & Technology. http://us.practicallaw.com/w-001-0073

ACRONYMS

ACL	Access Control List
ACS	Access Control System
AODB	Airport Operational Database
API	Application Programming Interface
ASC	Airport Security Coordinator
ASP	Airport Security Program/Plan
ATSA	Aviation Transportation Security Act
BCP	Business Continuity Plan
BES	Bulk Electric Systems
BICSI	Building Industry Consulting Service International
CBP	Customs and Border Protection
CCTA	Central Computer and Telecommunications Agency
CIA	Confidentiality, Integrity, and Availability
CMDB	Configuration Management Database
CMMS	Computerized Maintenance Management System
CRAMM	CCTA Risk Analysis and Management Method
CUPPS	Common Use Terminal Passenger Processing
CUTE	Common Use Terminal Equipment
DAS	Direct Attached Storage
DCS	Departure Control System
DISA	Defense Information Systems Agency
DRP	Disaster Recovery Plan
FAR	Federal Aviation Regulation
FIPS	Federal Information Processing Standards
GAO	Government Accountability Office
GIDS	Gate Information Display Systems
GRC	Governance, Risk Management, and Compliance
HVAC	Heating, Ventilation, and Air Conditioning
ICS	Incident Command System
ICP	Incident Command Post
IDM-CIS	Identity Management and Credentialing Systems
IDMS	Identity Management System
IDS/IPS	Intrusion Detection/Prevention Systems
IEC	International Electrotechnical Commission
ISMS	Information-Based Security Management System
ISO	International Organization for Standardization

LAN	Local Area Network
MAN	Metropolitan Area Network
NAC	Network Access/Admission Control
NAS	Network Attached Storage
NIMS	National Incident Management System
O&M	Operation and Maintenance
OOB	Out-of-Band
OSI	Open Systems Interconnection
PACS	Physical Access Control Systems
PBX	Private Branch Exchange
PIDS	Perimeter Intrusion Detection Systems
RFP	Request for Proposals
RFQ	Request for Qualification
SAN	Storage Area Network
SD	Security Directive
SIEM	Security Information and Event Management
SP	Special Publication
STIG	Security Technical Implementation Guide
TS SSP	Transportation Systems Sector-Specific Plan
TVA	Threat and Vulnerability Assessment
UL	Underwriters Laboratory
UV	Unmanned Vehicle
VLAN	Virtual Local Area Network
VMS	Video Management System
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WISP	Written Information Security Program

APPENDIX A: GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE (GRC) TOOLKIT

Securing access to vital systems impacting airport security starts with governance, risk management, and compliance. This toolkit provides a framework for documenting these systems and the physical places they reside, as well as guidance for managing and maintaining them. The parts of this toolkit include:

Governance

- Governance Charter and By-Laws
- Governance Organizational Chart
- Governance Organizational Chart with Project-Oriented Committee
- Governance Roles and Responsibilities

Risk Management

- Asset and Inventory Management
- Concept of Operations
- CRAMM Threat and Vulnerability Assessments/Risk Assessment Methodology
- Countermeasures

Compliance

- Written Information Security Program

Governance

This toolkit offers guidance to airport executive and IT leaders for developing a Governance Charter. Listed here are critical components of any Governance Charter along with sample statements and airport IT advisor recommendations. To use this toolkit, one should first review the recommendations and examples on the elements of a Governance Charter and then answer the questions at the end of this document to develop their own Governance Charter, reflective of the airport's needs.

IT/OPERATIONS GOVERNANCE CHARTER ELEMENTS

Below are listed some critical components of the Governance Charter. To provide an example of what each component looks like, we have compiled examples and recommendations from different charters. These are intended only to illustrate the possible contents of a charter, since not all organizations will choose to implement all of the components in the manner listed here.

ORGANIZATION AND STRUCTURE OF GOVERNANCE

Recommendation: Streamline governance structures with care to provide appropriate input without compromising the efficiency of decision making.

Rationale: The purpose of the governance structure is to provide an appropriate say in decision making to all parties affected by the work of Operations and IT. Some institutions find that a single IT/Operations Steering Committee is adequate to provide effective governance, while others require a more complex hierarchy of subcommittees. The need for subcommittees is determined by the volume and scope of the efforts undertaken by the airport. The greater the number of project requests, ongoing implementations, and scope of the security systems/physical spaces portfolio, the greater the need for delegation of responsibilities by the Steering Committee to various subcommittees. Business partnerships with external organizations that require close coordination of airport operations and IT may also necessitate the use of subcommittees. The greater the number of committee members, the more difficult it may be to schedule meetings and make decisions; consequently, each committee would ideally consist of between three and seven members, not including support staff. A large committee membership is a clear sign that a subcommittee structure should be considered. See Figures 17 and 18 below for examples of governance structures.

Once the components above have been reviewed, airports should consider the 10 questions listed below. The answers to these questions provide the framework for an Operations/Governance Charter

- □ What is the purpose of the Steering Committee?
- □ What are the roles and responsibilities of Steering Committee members?
- □ Who sits on the Steering Committee? Is this a rotating or permanent membership?
- □ At what frequency will the Steering Committee meetings take place?
- □ Are subcommittees required? If so, for what purposes?
- □ What is the organizing principle for subcommittees (for example: based on functional areas)?
- □ What are the roles and responsibilities of the various subcommittees?
- □ Who sits on each of the subcommittees?
- □ At what frequency will the subcommittees meet?
- □ Who will serve as the communication conduit between the subcommittees?

Governance Charter (Example)

COMMITTEE NAME:

GOVERNANCE COMMITTEE

CHARTER EFFECTIVE DATE AND DURATION:

January 1, 20xx – December 31, 20xx

COMMITTEE PURPOSE:
(The overall scope and focus of the committee description, including goals)

DELIVERABLES:
(Service, product, or document provided by the committee)

1. Committee Meeting Agendas and Minutes documents
2. Project-oriented business documents
3. Previous governance committee documents
4. Documents used for transitioning annual changes in governance committee
5. Governance committee member schedules and assignments

ADMINISTRATIVE AND REPORTING REQUIREMENTS:
(Reports to Governance Committee through whom, when, and how?)

1. Uses standard agenda, note-taking and reporting templates adopted by airport
2. Other Airport Committee Chairs report back to their respective committees after each Governance Committee Meeting

RESOURCES AND BUDGET:
(In terms of budget, staff, etc.)

COMMITTEE COMPOSITION AND TERMS:

- Governance Committee members are annually elected by the Board of Directors for a one-year term

VOLUNTEER REQUIREMENTS, EXPERIENCE, AND SKILLS:

Committee Specific:

- Must be a member of a subsequent committee

COMMITTEE CHAIR AND CONTACT INFORMATION:

Name:
E-mail Address:

COMMITTEE CHAIR ROLES AND RESPONSIBILITIES:

1. Keeps the committee focused on accomplishing the mission and objectives detailed in the charter.
2. Ensures all committee members are fully oriented on the committee objectives, deliverables and roles/ responsibilities at the committee's first meeting.
3. Works toward building a sense of trust, productivity, and camaraderie within the committee.
4. Develops meeting agendas.
5. Conducts meetings of the committee and directs the communication for committee matters.
6. Works to ensure that meeting notes capture consensus agreement items and follow-up actions of the committee using the standard meeting notes template.
7. Works with the Executive Liaison to review the charter mid-year and offer recommendations to Governance Committee for updates to the following year's charter.
8. Assigns tasks among committee members, as necessary.
9. Transitions the incoming Committee Chair into the role.

EXECUTIVE LIAISON ROLES AND RESPONSIBILITIES:

1. Supports the mission and objective of the committee through empowered decision making and discusses any policy violations with the Airport Executive Operator.
2. Works in coordination with the Committee Chair to efficiently discharge the responsibilities of the committee.
3. Works in coordination with the Committee Chair to develop agendas, set meeting dates and locations, and communicate meeting requirements using the following criteria:
    a. Meeting dates and locations should be determined as far in advance as possible.
    b. Meeting request forms should be sent to the proper contact with all meeting requirements stated.
    c. Agendas should be developed using the standard agenda template and should include the meeting date, venue, and meeting room on all agendas. The agenda should reflect what agenda items are tied to a stated deliverable in the charter.
    d. Handouts should be distributed to the team in advance of the meeting via the team's online community.
4. Works in coordination with the Committee Chair to capture notes that reflect consensus agreements and follow-up actions.

5. Works in coordination with the Committee Chair to ensure all reports, proposals, and supporting documentation are developed in a professional and timely manner.
6. Coordinates and deploys any approved external communications.

APPLICABLE GOVERNING DOCUMENTS:
(Specifically add airport-relevant governing documents)

1. PMI Code of Ethics and Professional Conduct
2. Bylaws
3. Policies and Procedures
4. Strategic Plan
5. Policy on Volunteerism
6. Policy on Conflict of Interest
7. Policy on Confidentiality

(Reference: http://www.pmi.org, Governance Committee Charter)

Figure 17. Example Operations/Governance Structure with Functionally Oriented Subcommittees

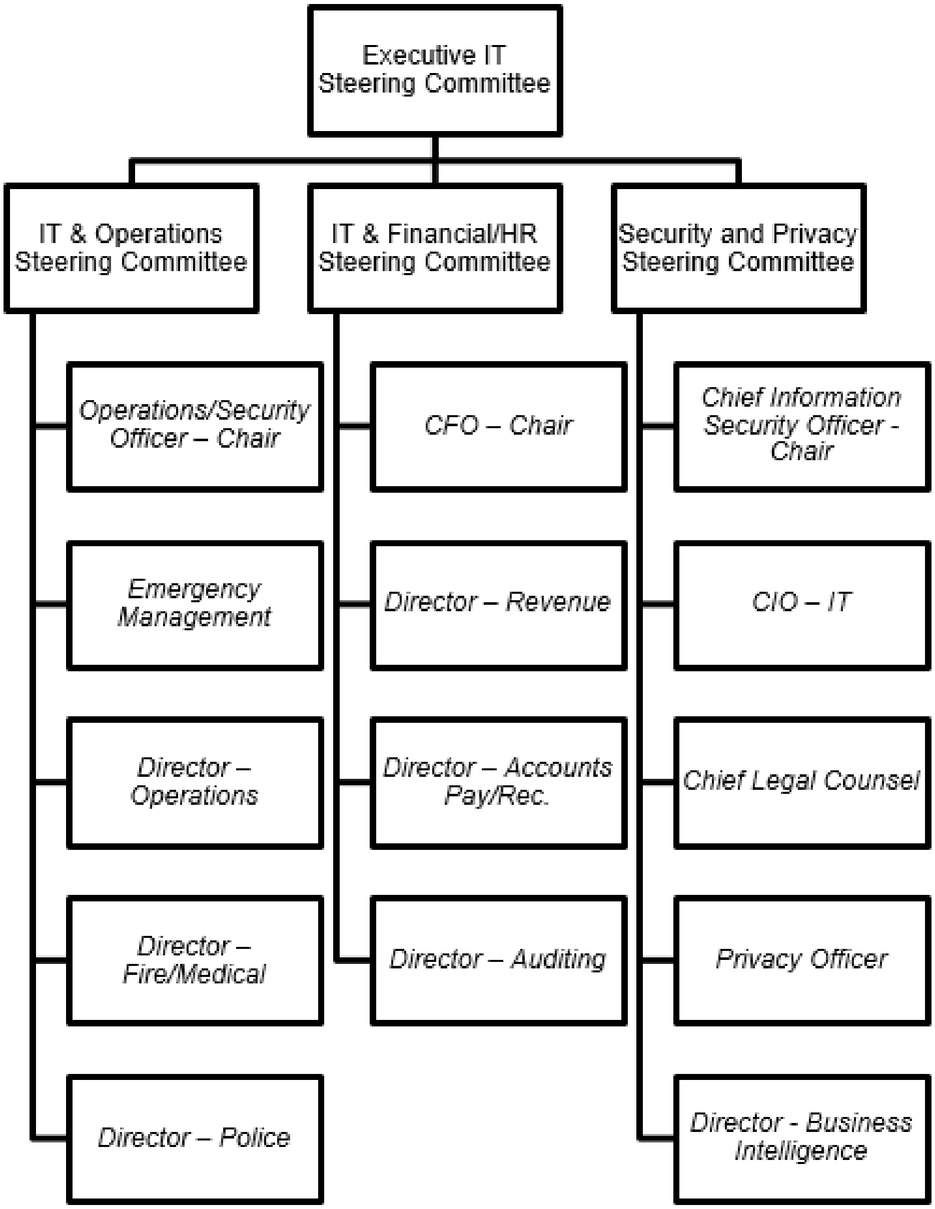
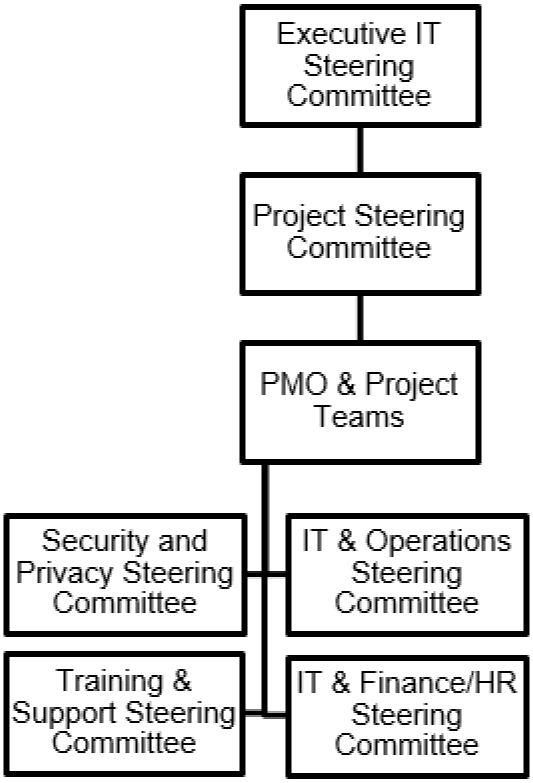

Executive IT Steering Committee
IT & Operations Steering Committee
IT & Financial/HR Steering Committee
Security and Privacy Steering Committee
Operations/Security Officer – Chair
Emergency Management
Director – Operations
Director – Fire/Medical
Director – Police
CFO – Chair
Director – Revenue
Director – Accounts Pay/Rec.
Director – Auditing
Chief Information Security Officer - Chair
CIO – IT
Chief Legal Counsel
Privacy Officer
Director - Business Intelligence

Figure 18. Example Operations/Governance Structure with Project Oriented Committee Structure


Executive IT Steering Committee
Project Steering Committee
PMO & Project Teams
Security and Privacy Steering Committee
IT & Operations Steering Committee
Training & Support Steering Committee
IT & Finance/HR Steering Committee

EXECUTIVE STEERING COMMITTEE

Focuses on strategy, monitoring execution, and being involved in an overview of the project's details (budget requests, change of scope, delays impacting other projects, etc.) The additional subcommittees should cover the checklist of items listed below.

□ Includes User and IT executive sponsors
□ Monitors a given project's execution (work plan, scope, budget, benefit realization)
□ Refers issues it cannot solve (within allotted budget and resources, and scope) to the Executive Steering Committee
□ Drives overall project work plan and tracks resources, effort, and funding
□ Manages project and tracking tools focusing on status, performance, and issues
□ Delivers the communication strategy
□ Manages budget and provides updates for funding support as needed

Recommendation: Each committee and subcommittee should have a purpose statement that can be used to refine the roles, responsibilities, and membership of the committee

Rationale: The purpose statement for each committee is the foundation for developing a list of roles and responsibilities, for determining membership, and for establishing meeting frequency

Examples:

Steering Committee purpose statement: The Operations/Governance Steering Committee provides guidance and oversight in planning, prioritizing, and implementing IT-enabled initiatives to improve the quality and efficiency of the organization's services to passengers, tenants, employees, and the community.

Subcommittee purpose statement: The Governance Subcommittee provides guidance and oversight in planning, prioritizing, and implementing IT-enabled initiatives in support of IT and Operational services.

COMMITTEE ROLES AND RESPONSIBILITIES

Recommendation: Clearly articulate the roles and responsibilities for each Governance Committee

Rationale: A key success factor for effective governance is clarity about roles and responsibilities of both the Steering Committee and the various subcommittees. A clear description of the authority of each committee can provide a compelling reason for committee members to participate, and can lead to higher levels of leadership engagement. Surveys show that the majority of governance processes are separate from other corporate planning processes in a typical provider organization. This can lead to confusion about oversight and decision making unless roles and responsibilities are clearly spelled out. Likewise, if the governance structure employs subcommittees, it is important to be clear about each committee's responsibilities.

Examples: The following is a sample list of possible roles and responsibilities for a Governance Steering Committee and Subcommittee. This list may be used as a starting point to develop an appropriate charter, though all of the items here may not apply to every organization.

Sample Steering Committee Roles and Responsibilities

- Approve organization-wide IT policies, procedures, and standards
- Oversee protocols to address any requests for exceptions to standards, or deviations from policy or standard procedures.
- Review and approve IT strategy and implementation plan
- Ensure alignment with enterprise strategy and plans
- Evaluate and prioritize the strategic IT-enabled initiatives based on predetermined criteria
- Review and approve allocation of IT resources for departmental efforts
- Ensure the identification of clear and measurable IT/Operational and business goals and objectives for the approved portfolio of work
- Establish clear individual leader accountabilities for achieving the planned outcome goals and objectives
- Ensure availability of all resources required for the approved portfolio of work (both IT and non-IT), matching the work approved to the capacity of the organization
- Assist in the development of an implementation plan with logical sequencing of efforts that minimizes the competition for the same resources
- Review and recommend IT-related investments for the Capital Allocation Committee
- Ensure the inclusion of appropriate levels of capital replacement funding, ideally through a refreshed budget
- Ensure appropriate funding for net new investments
- Monitor progress of the approved portfolio of work, intervening when necessary to alter plans or adjust resourcing
- Require regular progress updates from business and IT/Operations partners
- Assess progress towards planned outcome goals and objectives continuing oversight until the desired outcomes are achieved
- Guide course corrections if warranted by performance variance
- Regularly review developments in IT looking for new opportunities that can be leveraged by the organization
- Charter subcommittees or working groups as required to maintain effective governance

Sample Subcommittee Roles and Responsibilities

- Review and approve work plans for all work in the scope of the subcommittee as assigned by the Steering Committee
- Evaluate and rank the work within the committee's scope of responsibility
- Ensure availability of all resources required for the committee's scope of work (both IT and non-IT), matching the work to the allocation of resources approved by the Steering Committee
- Assist in the development of an implementation plan with a logical sequencing of efforts that minimizes the competition for the same resources
- Regularly review all work in the scope of the subcommittee
- Require regular progress updates from business and IT/Operations sponsors
- Assess progress towards project completion and toward planned outcome goals and objectives, continuing oversight until the desired outcomes are achieved
- Guide course corrections if warranted by performance variance, requesting Steering Committee assistance when necessary
- Review and recommend IT investments to the Steering Committee

MEMBERSHIP

Recommendation: Select committee members with the authority to fulfill the purpose of the committee

Rationale: A key factor in deciding membership is that each committee member should be prepared to be held accountable for the work approved by the committee. IT carries the additional burden of guiding and facilitating the processes of the committees.

Examples:

Steering Committee Membership: Board members, C-suite executives, Vice Presidents, or other key Senior Management Team members

Subcommittee Membership: Vice-Presidents, Directors, Managers, or other key staff members

MEETING FREQUENCY

Recommendation: Align committee meetings with the organization's planning cycle.

Rationale: Meeting frequency is generally determined by four organizational planning cycles: budget planning, capital investment planning, strategic planning, and work planning. Capital and operating budgets are typically revisited on an annual basis and strategies are generally reviewed annually but a new strategy may be required only once every 3-5 years. The broad sweep of IT responsibilities encompasses too many variables to create accurate work plans that extend beyond six months in most organizations. Consequently, work planning is most effective if plans are revisited multiple times per year.

Examples:

Steering Committee

- Quarterly meetings, at a minimum, are required to review budget proposals and work plans. However, the broader the scope and complexity of the work, the more frequently the Steering Committee should meet.
- The Steering Committee should plan to meet more frequently during years in which the Operations and/or IT strategy is being renewed.

Subcommittees

- In order to provide adequate and timely updates and information to the Steering Committee, subcommittees should meet at least as often as the Steering Committee.
- Generally, subcommittees find that the type of work they are accountable for requires meeting at least monthly if not weekly.

RISK MANAGEMENT

Asset/Inventory Management

A good asset/inventory management system contains information that is continually updated as equipment/assets go through their life cycle replacements. The following data, at a minimum, should be captured for each asset type:

- An inventory of all of the hardware components, including model numbers, purchase dates, end-of-life estimates, initial cost, and any additional pertinent information that is essential for understanding the characteristics of the hardware
- An inventory of all of the software components, including license information, expiration dates, patching requirements, acquisition cost, and system owner
- A detailed listing of all of the information that is maintained on these systems, its sensitivity and/or confidentiality, data storage location, and retention and disposal policy
- An architectural depiction of the specific system and its level of integration with other physical security systems
- A complete description of the underlying infrastructure that supports the physical security systems, likely focusing on the network, all of its components, and its management structure
- A description of the airport staff and contractual resources that support each system, including cost, contract expiration, and contract requirements

CCTA Risk Analysis and Management Method (CRAMM)

The following risk assessment tools and formulas (e.g., CCTA Risk Analysis and Management Method, CRAMM) are promoted by the IT Infrastructure Library (ITIL). ItSM Solutions DITY Weekly Newsletter from December 2008 provides a "10 Steps to Do It Yourself CRAMM" presented below. These can be used to identify the criticality of the airport's systems and physical spaces and components. Once known, these numbers can be added to the asset inventory line item for each component.

1. Grant authority for the security review to move forward

2. Define the scope of the review using the airport security areas and systems vital to airport security sections

3. Assign a team as defined in the governance section

4. Identify systems and their physical locations

5. Agree to the control types applicable

6. Start collecting data

7. Stage 1 - Identify assets within the scope of the review (data, application/software and physical assets.) A Configuration Management Database (CMDB) is a valuable software tool. If the

airport does not have a CMDB, then performing an inventory and capturing information on mission-critical data, software, and physical assets is essential.

Prepare a grid or table. A spreadsheet, as shown in Figure 19, works well for this. For each asset, list the asset and the asset owner—the owner is the person who knows best the usage and value of this asset. This process also raises the level of acceptance of your review findings and proposals.

Figure 19. CRAMM Example Form Used for Each System/Physical Location

Asset Owner: SAMple Airport
Name/Department: SAMple Parking Operations Manager

Asset: *Access Control System (ACS)*
Location: *Data Room 101 (SAMple Airport Terminal)*
Description: *The ACS handles all access to doors within the terminal and some outlying buildings. Other buildings not on the ACS are controlled by the CardKey or with Keyed locks and have their own CRAMM form.*

	CONFIDENTIALITY			INTEGRITY		AVAILABILITY	
	public (0) restricted (1–5) confidential (6–9) secure (10)			low (1–3) moderate (4–7) high (8–9) very high (10)		low (1–3) moderate (4–6) high (7–8) very high (9) mandatory (10)	
***Impact Requirement** (1–10)*	10/secure			10/very high		9/very high	
Threats list all that apply	Disclosure	Theft	Loss	Hacking	Input Errors	Physical Access to System	Power Failure
							Vulnerability (1-10)
none (0) low (1–4) moderate (5–7) high (8–9) very high (10)	10	3	1	8	2	8	8
							Threat (1 to 100)
Impact X Vulnerability = Risk Level	**100**	**30**	**10**	**80**	**20**	**72**	**72**
Low (1–33)	High	Low	Low	High	Low	High	High
Medium (34–67) High (68–100)							
***Countermeasures** list all that apply*	Password Protection Encryption	Physical Locks	Backup	Firewall	Data validation	Add Locks to Data Room or Access Control	Install Backup Power
					Data Input Forms		

8. Interview the asset owner; have the asset owner value data and software assets by the impact/cost resulting from loss of confidentiality, integrity, or availability; and physical assets by replacement cost. Have data owners consider the impact of the following attributes of their asset:

    a. Confidentiality – impact of or sensitivity to disclosure of the asset to non-authorized parties, e.g., “employees,” “contractors,” etc. Use confidentiality requirement categories of public (0), restricted (1–5), confidential (6–9), and secure (10).

    b. Integrity – impact of unknown or unauthorized modification e.g. “data input errors,” etc. Use integrity requirement categories of low (1–3), moderate (4–7), high (8–9), and very high (10).

    c. Availability – impact of the asset being unavailable for various time frames, e.g., “less than 15 minutes,” “1 hour,” “1 day,” etc. Use availability requirement categories of low (1–3), moderate [OK to recover in days] (4–6), high [hours] (7–8), very high [minutes] (9), and mandatory [cannot be down] (10).

    For a, and c above, have the data owner first choose a category for each, then a value within the category. For example, for Integrity, have them choose first from low, moderate, high and very high. Then, if they chose moderate in this case, ask them to rank the impact on a scale of 4 to 7.

    If there are existing measures already in place to control risks, identify them during this stage. Update the grid and move to Stage 2.

9. Stage 2: Review and agree on the results from Stage 1. Determine how likely each risk in Stage 1 is by asking questions of support personnel, experts, and other personnel using prepared questionnaires to try and assess the likelihood that the identified risks could occur. Consider hackers (inside and outside the airport), viruses, failures (hardware and software), disasters (terrorism and natural), and people, process, or procedure errors. Create a column for each threat. Use a category of none (0), low (1–4), moderate (5–7), high (8–9), and very high (10). Update the spreadsheet for each asset.

10. Calculate the Risk entry by multiplying the Impact by the Vulnerability. Based on the risk score (impact x vulnerability) assign a label of low (1–33), medium (34–67), or high (68–100). Update the spreadsheet for each asset. This produces a list of the areas having the most risk. Developing and approving this list through a Governance Committee should provide a strong basis for justifying the need to proceed.

11. Stage 3: Review and agree on the results from Stage 2. Begin to identify and select countermeasures for those assets with the highest risk level.

12. Consider countermeasures and ways to mitigate the threats. Focus on the higher-level threats first, but do not overlook quick, easy, or cheap fixes to lower level threats. Give precedence to those countermeasures that:

    - Protect against several threats
    - Protect high risk assets
    - Apply where there are no countermeasures already in use
    - Are less expensive to implement
    - Are more effective at preventing or mitigating threats
    - Prevent threats rather than detecting or facilitating recovery

- Can be implemented quickly, easily, and inexpensively (even for low risk)

The following templates are designed to focus on the types of information needed for assets and inventory pertaining to protecting access to systems impacting airport security. Free software is available to expedite this process with some examples presented below.

ASSET AND INVENTORY TEMPLATE (WITH SAMPLE DATA)

Unique ID	Name / Product	Description	Category	Dept. / Local	RM	Purchase Date	Manufacturer	Warranty Exp. Date	Cost	Model #.	Serial #.	Risk #	System / Resource Owner	Link to Documents	Link to Photos
1001	Gate Controller	Gate B-17	Physical ACS	Ops	n/a	12/1/2015	Tymetal Corp.	12/1/2025	$2500	G100	223233	10	Ops	Network	Network
1002	C-Cure 9000 Server	Access Control Server	ACS	IT	DC100	11/20/2013	Software House / Tyco	11/20/2018	$15,000	PE1500	123432	10	IT	Network	Network

For each asset in the Asset and Inventory Template above, fill out a Risk Assessment form as shown below. This CRAMM Form can also be used for physical security and data:

Asset Owner:
Name/Department:

Asset:
Location:
Description:

	CONFIDENTIALITY			INTEGRITY		AVAILABILITY	
	public (0) restricted (1–5) confidential (6–9) secure (10)			low (1–3) moderate (4–7) high (8–9) very high (10)		low (1–3) moderate (4–6) high (7–8) very high (9) mandatory (10)	
***Impact Requirement** (1–10)*							
Threats *list all that apply*							
							Vulnerability (1-10)
none (0) *low (1–4)* *moderate (5–7)* *high (8–9)* *very high (10)*							
							Threat (1 to 100)
Impact X Vulnerability =							
Risk Level							
Low (1–33)							
Medium (34–67) *High (68-100)*							
Countermeasures *list all that apply*							

More examples of simplified Risk Assessment forms:

#	Location/Hazard	Consequences	Risk Assessment			Mitigations	Residual Risk (if any)	Comments
			Likelihood	Severity	Result (RAC)			
1								
2								

Hazard #	Mitigation	Person(s) Responsible	Proposed Completion Date

APPENDIX B: SECURITY CONTROLS AND COUNTERMEASURES MATRIX

In order to develop the necessary controls for a specific airport environment, it is important to understand the different control categories and how each may fit into an airport's operating environment. Airports may find it advantageous to borrow controls from other airports, and then modify those controls to fit their operating circumstances and environment. This matrix was created to assist the airport operator with developing a baseline of security controls for vital systems, networks, and physical elements impacting airport security.

Security Controls Matrix

	Directive	Deterrent	Preventative	Compensating	Detective	Corrective	Recovery
	Directive controls specify acceptable rules of behavior	*Deterrent controls discourage people from violating airport policies or directives*	*Preventive controls prevent a security incident or breach*	*Compensating controls mitigate the loss of primary controls and reduce risk to an acceptable level*	*Detective controls issue a warning when a security control has been violated or breached*	*Corrective controls mitigate damage, or restore controls*	*Recovery controls restore conditions to normal after a security incident*
Response Type	Preventative				Response		

Physical Locks and Keys

	Directive	Deterrent	Preventative	Compensating	Detective	Corrective	Recovery
Administrative	Policy	Employee shares Key, Key immediately revoked	Policy indicating background check be performed	All personnel without Keys will be escorted	Spot checking of Key usage or checking historical CCTV footage	Any employee found violating policy will be suspended and/or terminated	All Key assignments will be logged and Key checks conducted
Technical	If Cyberlock – Core reprogramming due to lost key	Video Surveillance of Keyed Location	Video Surveillance of Keyed Location	Secondary Key Lock or Access Control Method	All Key assignments will be logged and Key checks conducted	If Cyberlock – Core reprogramming due to lost key	Key inventory conducted
Physical	"Do Not Enter Without Authorization" Sign	"Do Not Enter Without Authorization" Sign	N/A	All security systems will be protected through multiple	CCTV will be employed at the entry to all data centers and	N/A	Locks will be re-cored, Keys re-issued

				defense mechanisms, including locks, cages, and locked racks.	communication rooms that house physical security systems.		

Premises Distribution Systems (PDS)

	Directive	Deterrent	Preventative	Compensating	Detective	Corrective	Recovery
Administrative	Airport Design Standards Airport policy on access to PDS locations, including airport communication rooms, data centers, outside plants, and/or enclosures with PDS equipment (e.g., PDS Secured Areas)	Employees found sharing their credentials, user identification, and/or password, to PDS secured areas with any other individual will have all system rights immediately revoked	A policy that requires all contract personnel to be cleared through a background check process before being allowed to work on PDS	Badged airport personnel must escort all contract personnel when working on airport PDS	All attempts to enter a restricted area within the PDS with an unauthorized badge will be recorded in the system's security log and all logs reviewed at least weekly. Key-controlled areas will have access logs reviewed at least weekly.	Any employee found violating policy will be suspended and/or terminated	Airport Operator will have on-call repair technicians for PDS repairs (e.g., fiber, conduit) The airport will maintain an updated disaster recovery plan at all times, with periodic testing no less than every 6 months
Technical	Administrative passwords on all security system routers, switches and controllers must be changed every 30 days.	When logging on to airport physical security system routers, switches, or controllers, a warning banner is displayed that states only authorized personnel may attempt access to the system.	All airport communication rooms that house PDS components must use both an automated access control mechanism (swipe card) and a PIN.	Facial recognition analytics will be employed at the entry to any PDS area.	Detailed logs will be maintained for all PDS locations for a minimum of 90 days.	Any PDS components, such as routers, switches, and controllers, will have hot spares available for swap out.	All PDS components such as routers, switches, and controllers will have a back-up schedule with a recovery point objective of not more than 4 hours.

Physical	"Do Not Enter without Authorization" signs are placed on the entry to all airport communication rooms, data centers, outside plants, and enclosures housing PDS equipment.	A sign is posted on a controlled door that states only authorized personnel may enter, and a violator that engages the alarm may be subject to criminal prosecution.	All PDS components such as routers, switches, and controllers are stored in the airport communications rooms, data centers, outside plants, and enclosed housings and the "least privilege" concept applies to access	All PDS components will be protected through multiple defense mechanisms, including locks, cages, and locked racks.	CCTV will be employed at the entry to all PDS locations, such as data centers and communication rooms that house physical security systems.	Alarm and control sensors on PDS components and in PDS locations can be programed so that mitigation plans can occur.	The airport will maintain a Disaster Recovery "hot-site" for all physical security systems on the PDS that can be activated within one hour of a major disaster. One example includes using wireless communications to reroute systems.

Data Center and Associated Hardware

	Directive	Deterrent	Preventative	Compensating	Detective	Corrective	Recovery
Administrative	Same as PDS	Same as PDS	Same as PDS	Same as PDS	Same as PDS	Same as PDS	Same as PDS
Technical	Same as PDS	Same as PDS	Same as PDS	Same as PDS	Same as PDS	Same as PDS	Same as PDS
Physical	Same as PDS	Same as PDS	Same as PDS	Same as PDS	Same as PDS	Same as PDS	Same as PDS

ID Badging & Credentialing System (IDMS)

	Directive	Deterrent	Preventative	Compensating	Detective	Corrective	Recovery
Administrative	Airport employees may not share ID Badge holder or access control data from the airport's IDMS without express written approval of the public safety department.	Employees found sharing their ID badge, user identification and/or password with any other individual will have all IDMS rights immediately revoked.	A policy that requires all contract personnel to be cleared through a background check process before being allowed to work on IDMS.	Badged airport personnel must escort all contract personnel when working on IDMS, unless contract personnel are badged.	All attempts to enter a restricted area with an unauthorized badge will be recorded in the system's security log and all logs reviewed at least weekly.	Any airport employee found violating the Third Party User Policy and/or the Computer Use policy will be suspended upon first violation and terminated on any subsequent violation.	The airport will maintain an updated disaster recovery plan at all times, with periodic testing no less than every 6 months

Technical	Administrative passwords on all security system, including IDMS must be changed every 30 days.	When logging on to an airport IDMS, a warning banner is displayed that states only authorized personnel may attempt access to the system.	All airport communication rooms that house IDMS must use both an automated access control mechanism (swipe card) and a pin.	Alternate forms of two-factor authentication for access to IDMS (e.g., biometric). IDMS will have redundant and/or fail-over server (e.g., hybrid or cloud-based). All IDMS data containing PII and/or SSI must be encrypted in transit and at rest.	Detailed logs will be maintained for all physical security systems for a minimum of 90 days.	Any IDMS desktop workstation that is suspected of containing malware of any sort will be immediately unplugged from the airport network and may not return to the network until it has been thoroughly investigated and "cleaned" by the IT department.	All IDMS will have a back-up schedule with a recovery point objective of not more than 4 hours
Physical	"Do Not Enter without Authorization" signs are placed on the entry to all airport communication rooms and locations where IDMS resides.	A sign is posted on a controlled door that states only authorized personnel may enter, and a violator that engages the alarm may be subject to criminal prosecution.	All IDMS are stored in separate caged areas in the airport's data centers and the "least privilege" concept applies to access.	All IDMS will be protected through multiple defense mechanisms, including locks, cages, and locked racks.	Video surveillance will be employed at the entry to all data centers and communication rooms that house IDMS.	A hot spare or fail over redundant will be available. A cold spare can also be included here.	A hot spare or fail over redundant will be available. A cold spare can also be included here.

Local Area Networks (LAN)

	Directive	Deterrent	Preventative	Compensating	Detective	Corrective	Recovery

Administrative	Airport Design Standards Airport policy on access to LAN locations, including airport communication rooms, data centers, outside plants, and/or enclosures with LAN equipment.	Employees found sharing their credentials, user identification, and/or password to LAN secured areas with any other individual will have all system rights immediately revoked.	A policy that requires all contract personnel to be cleared through a background check process before being allowed to work on LAN.	Badged airport personnel must escort all contract personnel when working on airport LAN.	All attempts to enter a restricted area within the LAN with an unauthorized badge will be recorded in the system's security log and all logs reviewed at least weekly. Key controlled areas will have access logs reviewed at least weekly.	Any employee found violating policy will be suspended and/or terminated.	Airport Operator will have on-call repair technicians for LAN repairs (e.g., firewalls, routers, load balancers, demarks, racks, and cabling) The airport will maintain an updated disaster recovery plan at all times, with periodic testing no less than every 6 months.
Technical	Administrative passwords on all LAN components such as firewalls, routers, load balancers, switches, servers, and SAN/DAS/NAS must be changed every 30 days.	When logging on to airport LAN components such as firewalls, routers, load balancers, switches, servers, and SAN/DAS/ NAS, a warning banner is displayed that states only authorized personnel may attempt access to the system.	All airport communication rooms that house LAN components must use both an automated access control mechanism (swipe card) and a pin.	Alternate paths for data and telecommunications will be established for LAN resiliency.	Detailed electronic logs will be maintained for all LAN locations for a minimum of 90 days from LAN components such as firewalls, routers, load balancers, switches, servers, and SAN/DAS/NAS	Any LAN components such as firewalls, routers, load balancers, switches, servers, and SAN/DAS/NAS will have hot spares available for swap out.	All LAN components such as firewalls, routers, load balancers, switches, servers, and SAN/DAS/NAS, will have a back-up schedule with a recovery point objective of not more than 4 hours.
Physical	"Do Not Enter without Authorization" signs are placed on the entry to	A sign is posted on a controlled door that states only authorized personnel may	All LAN components such as routers, switches, and controllers are	All LAN components will be protected through multiple defense	Video surveillance will be employed at the entry to all LAN locations,	Alarm and control sensors on LAN components and in LAN locations	The airport will maintain a Disaster Recovery "hot-site" for all LAN

	all airport LAN communication rooms, data centers, outside plants, and enclosures housing LAN equipment.	enter, and a violator that engages the alarm may be subject to criminal prosecution.	stored in the airport communications rooms, data centers, outside plants, and enclosed housings, and the “least privilege” concept applies to access.	mechanisms, including locks, cages, and locked racks.	such as data centers and communication rooms that house physical security systems.	can be programmed so that mitigation plans can occur.	components that can be activated within one hour of a major disaster. One example includes using wireless communications to reroute systems.

Physical Storage Devices

	Directive	Deterrent	Preventative	Compensating	Detective	Corrective	Recovery
Administrative	Airport employees may not share access to the airport’s physical storage devices without express written approval of the public safety department.	Employees found sharing their access to the airport’s physical storage devices with any other individual will have all system rights immediately revoked.	A policy that requires all contract personnel to be cleared through a background check process before being allowed to work on or have access to physical storage devices.	Badged airport personnel must escort all contract personnel when working on physical storage devices.	All attempts to enter a physical storage device with unauthorized access credentials will be recorded in the system’s security log and all logs reviewed at least weekly.	Any airport employee found violating the third-party user policy or the computer use policy will be suspended upon first violation and terminated on any subsequent violation.	The airport will maintain an updated disaster recovery plan at all times, with periodic testing of physical storage devices no less than every six months.
Technical	Written policy on access to physical storage devices.	When logging on to an airport physical storage device, a warning banner is displayed that states only authorized personnel may attempt access to the system.	All airport communication rooms that house physical storage devices must use both an automated access control mechanism (swipe card) and a pin.	Alternative access to physical storage devices should be created and used during an emergency.	Detailed logs will be maintained for all physical storage devices for a minimum of 90 days.	Any physical storage device that is suspected of containing malware will be immediately unplugged from the airport network and may not return to the network until it has been thoroughly	All physical security systems will have a back-up schedule with a recovery point objective of not more than 4 hours

						investigated and “cleaned” by the IT department.	
Physical	“Do Not Enter without Authorization” signs are placed on the entry to all airport communication rooms where physical storage devices reside.	A sign is posted on a controlled door that states only authorized personnel may enter and a violator that engages the alarm may be subject to criminal prosecution.	All physical security systems are stored in separate caged areas in the airport’s data centers and the “least privilege” concept applies to access.	All physical storage devices in security systems will be protected through multiple defense mechanisms, including locks, cages, and locked racks.	Video surveillance will be employed at the entry to all data centers and communication rooms that house physical storage devices.	A hot spare or fail over redundant will be available. A cold spare can also be included here.	A hot spare or fail over redundant will be available. A cold spare can also be included here.

Physical Access Control Systems (PACS)

	Directive	Deterrent	Preventative	Compensating	Detective	Corrective	Recovery
Administrative	Airport employees may not share video images or access control data from the airport’s PACS without express written approval of the public safety department.	Employees found sharing video images or access control data with any other individual will have all PACS rights immediately revoked.	A policy that requires all contract personnel to be cleared through a background check process before being allowed to work on PACS.	Badged airport personnel must escort all contract personnel when working on PACS.	All attempts to enter a restricted area with an unauthorized badge will be recorded in the system’s security log and all logs reviewed at least weekly.	Any airport employee found violating the Third-Party User Policy and/or the Computer Use policy will be suspended upon first violation and terminated on any subsequent violation.	The airport will maintain an updated disaster recovery plan at all times, with periodic testing no less than every 6 months.
Technical	Administrative passwords on all security systems must be changed every 30 days.	When logging on to an airport PACS, a warning banner is displayed that states only authorized personnel may attempt access to the system.	All airport communication rooms that house PACS must use both an automated access control mechanism (swipe card) and a pin.	Alternate forms of two-factor authentication for access to PACS (e.g., biometric). PACS will have redundant and/or fail-over server (e.g.,	Detailed logs will be maintained for all physical security systems for a minimum of 90 days.	Any PACS desktop workstation that is suspected of containing malware will be immediately unplugged from the airport network and	All PACS will have a back-up schedule with a recovery point objective of not more than 4 hours.

				hybrid or cloud-based).		may not return to the network until it has been thoroughly investigated and "cleaned" by the IT department.	
Physical	"Do Not Enter without Authorization" signs are placed on the entry to all airport communication rooms and locations where PACS resides.	A sign is posted on a controlled door that states only authorized personnel may enter, and a violator that engages the alarm may be subject to criminal prosecution.	All PACS are stored in separate caged areas in the airport's data centers and the "least privilege" concept applies to access.	All PACS will be protected through multiple defense mechanisms, including locks, cages, and locked racks.	Video surveillance will be employed at the entry to all data centers and communication rooms that house PACS.	A hot spare or fail over redundant will be available. A cold spare can also be included here.	A hot spare or fail over redundant will be available. A cold spare can also be included here.

Perimeter Intrusion Detection Systems (PIDS)

	Directive	Deterrent	Preventative	Compensating	Detective	Corrective	Recovery
Administrative	Airport employees may not share video images or access control data from the airport's PIDS without express written approval of the public safety department.	Employees found sharing video images or access control data with any other individual will have all PIDS rights immediately revoked.	A policy that requires all contract personnel to be cleared through a background check process before being allowed to work on PIDS.	Badged airport personnel must escort all contract personnel when working on PIDS.	All attempts to enter a restricted area with an unauthorized badge will be recorded in the system's security log and all logs reviewed at least weekly.	Any airport employee found violating the Third-Party User Policy and/or the Computer Use policy will be suspended upon first violation and terminated on any subsequent violation.	The airport will maintain an updated disaster recovery plan at all times, with periodic testing no less than every six months.
Technical	Administrative passwords on all security systems must be changed every 30 days.	When logging on to an airport PIDS, a warning banner is displayed that states only	All airport communication rooms that house PIDS must use both an automated	Alternate forms of two-factor authentication for access to PIDS (e.g., biometric).	Detailed logs will be maintained for all physical security systems for a minimum of 90 days.	Any PIDS desktop workstation that is suspected of containing malware will be	All PIDS will have a back-up schedule with a recovery point objective of not

		authorized personnel may attempt access to the system.	access control mechanism (swipe card) and a pin.	PIDS will have redundant and/or fail-over server (e.g., hybrid or cloud-based).		immediately unplugged from the airport network and may not return to the network until it has been thoroughly investigated and "cleaned" by the IT department.	more than 4 hours.
Physical	"Do Not Enter without Authorization" signs are placed on the entry to all airport communication rooms and locations where PIDS resides.	A sign is posted on a controlled door that states only authorized personnel may enter, and a violator that engages the alarm may be subject to criminal prosecution.	All PIDS are stored in separate caged areas in the airport's data centers and the "least privilege" concept applies to access.	All PIDS will be protected through multiple defense mechanisms, including locks, cages, and locked racks.	Video surveillance will be employed at the entry to all data centers and communication rooms that house PIDS.	A hot spare or fail over redundant will be available. A cold spare can also be included here.	A hot spare or fail over redundant will be available. A cold spare can also be included here.

Airport Operations Systems

	Directive	Deterrent	Preventative	Compensating	Detective	Corrective	Recovery
Administrative	Airport employees may not share video images or access control data from the airport's operation systems without express written approval of the public safety department.	Employees found sharing video images or access control data with any other individual will have all airport operations systems rights immediately revoked.	A policy that requires all contract personnel to be cleared through a background check process before being allowed to work on airport operation systems.	Badged airport personnel must escort all contract personnel when working on airport operations systems.	All attempts to enter a restricted area with an unauthorized badge will be recorded in the system's security log and all logs reviewed at least weekly.	Any airport employee found violating the Third-Party User Policy and/or the Computer Use policy will be suspended upon first violation and terminated on any subsequent violation.	The airport will maintain an updated disaster recovery plan at all times, with periodic testing no less than every six months.

Technical	Administrative passwords on all security systems must be changed every 30 days.	When logging on to an airport operation system, a warning banner is displayed that states only authorized personnel may attempt access to the system.	All airport communication rooms that house airport operation systems must use both an automated access control mechanism (swipe card) and a pin.	Alternate forms of two-factor authentication for access to airport operation systems (e.g., biometric). Airport operation systems will have redundant and/or fail-over server (e.g., hybrid or cloud-based).	Detailed logs will be maintained for all airport operation systems for a minimum of 90 days.	Any airport operation system desktop workstation that is suspected of containing malware will be immediately unplugged from the airport network and may not return to the network until it has been thoroughly investigated and "cleaned" by the IT department.	All airport operation systems will have a back-up schedule with a recovery point objective of not more than 4 hours.
Physical	"Do Not Enter without Authorization" signs are placed on the entry to all airport communication rooms and locations where airport operation systems reside.	A sign is posted on a controlled door that states only authorized personnel may enter, and a violator that engages the alarm may be subject to criminal prosecution.	All airport operation systems are stored in separate caged areas in the airport's data centers and the "least privilege" concept applies to access.	All airport operation systems will be protected through multiple defense mechanisms, including locks, cages, and locked racks.	Video surveillance will be employed at the entry to all data centers and communication rooms that house airport operation systems.	A hot spare or fail over redundant will be available. A cold spare can also be included here.	A hot spare or fail over redundant will be available. A cold spare can also be included here.

Security Information and Event Management (SIEM)

	Directive	Deterrent	Preventative	Compensating	Detective	Corrective	Recovery
Administrative	Airport employees may not share video images or access control data from the SIEM systems without express	Employees found sharing video images or access control data with any other individual will have all airport	A policy that requires all contract personnel to be cleared through a background check process before being	Badged airport personnel must escort all contract personnel when working on SIEM systems	All attempts to enter a restricted area with an unauthorized badge will be recorded in the system's security log and	Any airport employee found violating the Third-Party User Policy and/or the Computer Use policy will be suspended upon	The airport will maintain an updated disaster recovery plan at all times, with periodic testing

	written approval of the public safety department.	operations systems rights immediately revoked.	allowed to work on SIEM systems.		all logs reviewed at least weekly.	first violation and terminated on any subsequent violation.	no less than every six months
Technical	Administrative passwords on all security systems must be changed every 30 days.	When logging on to a SIEM system, a warning banner is displayed that states only authorized personnel may attempt access to the system.	All airport communication rooms that house SIEM systems must use both an automated access control mechanism (swipe card) and a pin.	Alternate forms of two-factor authentication for access to SIEM systems (e.g., biometric). SIEM systems will have redundant and/or fail-over server (e.g., hybrid or cloud-based).	Detailed logs will be maintained for all SIEM systems for a minimum of 90 days.	Any SIEM desktop workstation that is suspected of containing malware will be immediately unplugged from the airport network and may not return to the network until it has been thoroughly investigated and “cleaned” by the IT department.	All SIEM systems will have a back-up schedule with a recovery point objective of not more than 4 hours.
Physical	“Do Not Enter without Authorization” signs are placed on the entry to all airport communication rooms and locations where SIEM systems reside.	A sign is posted on a controlled door that states only authorized personnel may enter, and a violator that engages the alarm may be subject to criminal prosecution.	All SIEM systems are stored in separate caged areas in the airport’s data centers and the “least privilege” concept applies to access.	All SIEM systems will be protected through multiple defense mechanisms, including locks, cages, and locked racks.	Video surveillance will be employed at the entry to all data centers and communication rooms that house SIEM systems.	A hot spare or fail over redundant will be available. A cold spare can also be included here.	A hot spare or fail over redundant will be available. A cold spare can also be included here.

APPENDIX C: WRITTEN INFORMATION SECURITY PROGRAM (DOCUMENT TEMPLATE AND GUIDANCE)

The following Written Information Security Program (WISP) template follows the example supplemental document created and available for purchase from BlackHat Consultants, LLC. All Rights Reserved. 2016.

The WISP template follows the NIST 800-53 framework for creating a NIST-based Information Security Management System (ISMS).

INTRODUCTION/PURPOSE/SCOPE

The WISP provides definitive information on the prescribed measures used to establish and enforce the information security program. The purpose of the WISP is to prescribe a comprehensive framework for:

- Creating a NIST-based ISMS
- Protecting the confidentiality, integrity, and availability (CIA) of the airport's data and systems
- Protecting the airport, its employees, and its clients from illicit use of airport systems and data
- Ensuring the effectiveness of security controls over data and systems that support the airport's operations
- Recognizing the highly networked nature of the current computing environment and providing effective company-wide management and oversight of those related information security risks
- Providing for the development, review, and maintenance of minimum security controls required to protect the airport's data and systems

POLICY OVERVIEW, VIOLATIONS, EXCEPTIONS, & UPDATES

Airport users are required to protect and ensure the CIA of data and systems, regardless of how it data is created, distributed, or stored.

- Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system
- Security controls must be designed and maintained to ensure compliance with all legal requirements

Any user found to have violated any policy, standard, or procedure may face disciplinary action.

Exceptions to standards and/or policies occasionally occur and can be found in the Information Security Exception Request Procedures.

Updates to the WISP can be noted in this section, including the record of changes.

POLICIES, STANDARDS, PROCEDURES, & GUIDELINES STRUCTURE

This section covers the airport operator's policy, standards, procedures, and guidelines structure. For example, information security documentation is composed of five main parts: a core policy; a control objective that identifies desired conditions; measurable standards used to quantify the requirement; procedures that must be followed; and guidelines that are recommended, but not mandatory.

INFORMATION SECURITY CONTROL OBJECTIVES

Following NIST 800-53 guidelines, the airport's standards are organized into classes and families for ease of use in the control selection and specification process.

PROGRAM

- Focus is on information security program-level security topics
- Focus is on the overall framework for the program to govern management, operational, technical and privacy controls

MANAGEMENT

- Focus is on techniques and concerns that are normally addressed by management in the airport's information security program
- Focus is on the management of the information security program and the management of risk within the airport

OPERATIONAL

- Focus is on techniques and concerns that are generally implemented and executed by people, as opposed to systems that are put in place to improve the security of a particular system or group of systems
- These often require technical or specialized expertise, often relying upon management activities as well as technical controls

TECHNICAL

- Focus is on processes and technologies that computer systems control or execute
- These depend upon the proper functioning of the system for their effectiveness and therefore require significant operational considerations

PRIVACY

- Focus is on controls that impact Personally Identifiable Information (PII)
- These depend upon the proper functioning of the other classes of controls for their effectiveness, and therefore require significant operational considerations

A well-written WISP covers the following Control Areas:

- Common Controls
  - Program Management
- Management Controls
  - Awareness & Training
  - Personnel Security
  - Planning
  - Risk Assessment
  - System & Service Acquisition
- Operational Controls
  - Certification, Accreditation & Security Assessment
  - Contingency Planning
  - Incident Response
  - Maintenance
  - Media Protection
  - Physical & Environmental Protection
- Technical Controls
  - Access Control
  - Audit & Accountability
  - Configuration Management

  - Identification & Authentication
  - System & Communication Protection
  - System & Information Integrity
- Privacy Controls
  - Authority & Purpose
  - Data Accountability, Audit, & Risk Management
  - Data Quality & Integrity
  - Data Minimization & Retention
  - Individual Participation & Redress
  - Data Security
  - Data Transparency
  - Data-Use Limitations