PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY



PARAS 0067 October 2026

Guidance for IDMS Transitions

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Ann Barry
Dustin Danflous
Chris Runde
Introba, Inc.
St. Louis, MO

Saurabh Pethe
Eleanor Robichaud
Emily Baskin
Dean Hopkins
Kinexis Consulting, Inc.
Parsippany, NJ

Don Zoufal
Crowznest Consulting
Chicago, IL

© 2026 National Safe Skies Alliance, Inc. All rights reserved.

COPYRIGHT INFORMATION

Authors herein are responsible for the authenticity of their materials and for obtaining written permissions from publishers or persons who own the copyright to any previously published or copyrighted material used herein.

National Safe Skies Alliance, Inc. (Safe Skies) grants permission to reproduce material in this publication for classroom and not-for-profit purposes. Permission is given with the understanding that none of the material will be used to imply Safe Skies or Federal Aviation Administration (FAA) endorsement of a particular product, method, or practice. It is expected that those reproducing the material in this document for educational and not-for-profit uses will give appropriate acknowledgment of the source of any reprinted or reproduced material. For other uses of the material, request permission from Safe Skies.

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 their perimeter and access control security.

Through the ASSIST (Airport Security Systems Integrated Support Testing) 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 security technologies and procedures.

Through the POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), 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 of 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 PARAS Program Manager*

PARAS 0067 PROJECT PANEL

Jamie Hansen *AirBadge*
Nicole Jackson *Memphis International Airport*
Joseph Gaudio Jr. *AirTera*
David Brunjes *Port Authority of NY & NJ*
Melyssa Meuli *Metropolitan Airports Commission*
Jacquetta Charity *Metropolitan Washington Airports Authority*
Christy Russell *Dallas Fort Worth International Airport*
Ebenezer Henry *Aspen/Pitkin County Airport*
Michael DeVault *Burns & McDonnell*
Phaedra Fatuesi *Seattle-Tacoma International Airport*

AUTHOR ACKNOWLEDGMENTS

The PARAS 0067 research team would like to thank the many airport security professionals, badging offices, information technology personnel, procurement and legal representatives, access control administrators, and vendor implementation teams who supported the interview process and provided valuable perspectives on planning, procurement, cybersecurity, system integration, operational continuity, training, and long-term IDMS management. The willingness of participating organizations to share candid experiences, implementation challenges, lessons learned, and operational practices was critical to the development of this research and the practical guidance reflected throughout the PARAS 0067 – Guidance for IDMS Transitions report.

In addition, the research team would like to thank the Safe Skies PARAS program, which provided funding for this project. Particular thanks are given to the program manager, Jessica Grizzle, the PARAS program staff, and the project panel members for their guidance, feedback, and support throughout the research process. Their input helped strengthen the development of the report and ensure the guidance remained practical, relevant, and aligned with current airport operational environments.

CONTENTS

SECTION 1: INTRODUCTION 1
1.1 Purpose and Research Objectives 1
1.2 Scope of Research 1
1.3 Research Approach and Methodology 2
1.4 Airport and Stakeholder Participation 2
SECTION 2: OVERVIEW OF IDMS TRANSITIONS 3
2.1 Role of IDMS in Airport Operations and Security 3
2.2 Common Drivers for IDMS Transition 3
2.3 Industry Trends and Modernization 4
SECTION 3: NEEDS ASSESSMENT 6
3.1 Current-State Evaluation and Gap Analysis 6
3.2 Stakeholder Identification 9
3.3 Business Case Development 11
SECTION 4: SYSTEM REQUIREMENTS 13
4.1 Functional Requirements 13
4.2 Technical Requirements 14
4.3 Regulatory and Compliance Requirements 16
4.4 Performance Requirements 17
SECTION 5: PROCUREMENT CONSIDERATIONS 19
5.1 Procurement Strategy 19
5.2 Solicitation Structure 21
5.3 Vendor Evaluation Criteria 23
5.4 Demonstrations and Proof of Concept 24
SECTION 6: TRANSITION PROCESS 26
6.1 Transition Planning 26
6.2 Data Migration Strategy 28
6.3 System Integration and Testing 31
6.4 Operational Continuity 32
6.5 Cutover and Go-Live 34
SECTION 7: CONTRACT CONSIDERATIONS AND LEGAL ISSUES 36
7.1 Procurement and Contracting Law 36
7.2 Regulatory and CIP Compliance 37
7.3 Cybersecurity and Data Protection 38
7.4 Vendor Access and Control Rights 41
7.5 Operational Risk and Liability During Transition 42
SECTION 8: TRAINING AND DOCUMENTATION 45
8.1 Training Program Development 45

8.2 Documentation Requirements 46
8.2 Change Management 47
8.4 Ongoing Support and Knowledge Retention 49
SECTION 9: UPDATES TO PARAS 0038 – AIRPORT GUIDANCE FOR IDMS 51
9.1 Addition of New Subsections 51
9.2 Revise Existing Sections 52
9.1 Expand Existing Guidance 53
9.4 Final Observations 54
APPENDIX A: QUESTIONS FOR VENDOR INTERVIEWS A-1
APPENDIX B: QUESTIONS FOR LEGAL ISSUES INTERVIEWS B-1
APPENDIX C: QUESTIONS FOR AIRPORT INTERVIEWS C-1
APPENDIX D: CURRENT STATE EVALUATION CHECKLIST D-1
APPENDIX E: DATA MIGRATION STRATEGY CHECKLIST E-1
APPENDIX F: OPTIMIZED IDMS TRANSITION ROADMAP F-1

TABLES & FIGURES

Table 1. Documenting Evidence of Transition Needs 6
Table 2. Common Challenges and Goals Associated with IDMS Transitions 7
Table 3. Key Components of Data Migration Strategy During IDMS Implementation 29
Table 4. Key Factors for Operational Continuity During IDMS Transitions 33
Table 5. Cybersecurity and Data Protection Considerations for IDMS Transitions 39
Table 6. Proposed Additions to PARAS 0038 51
Table 7. Proposed Revisions to PARAS 0038 52
Table 8. Proposed Expansions to PARAS 0038 53

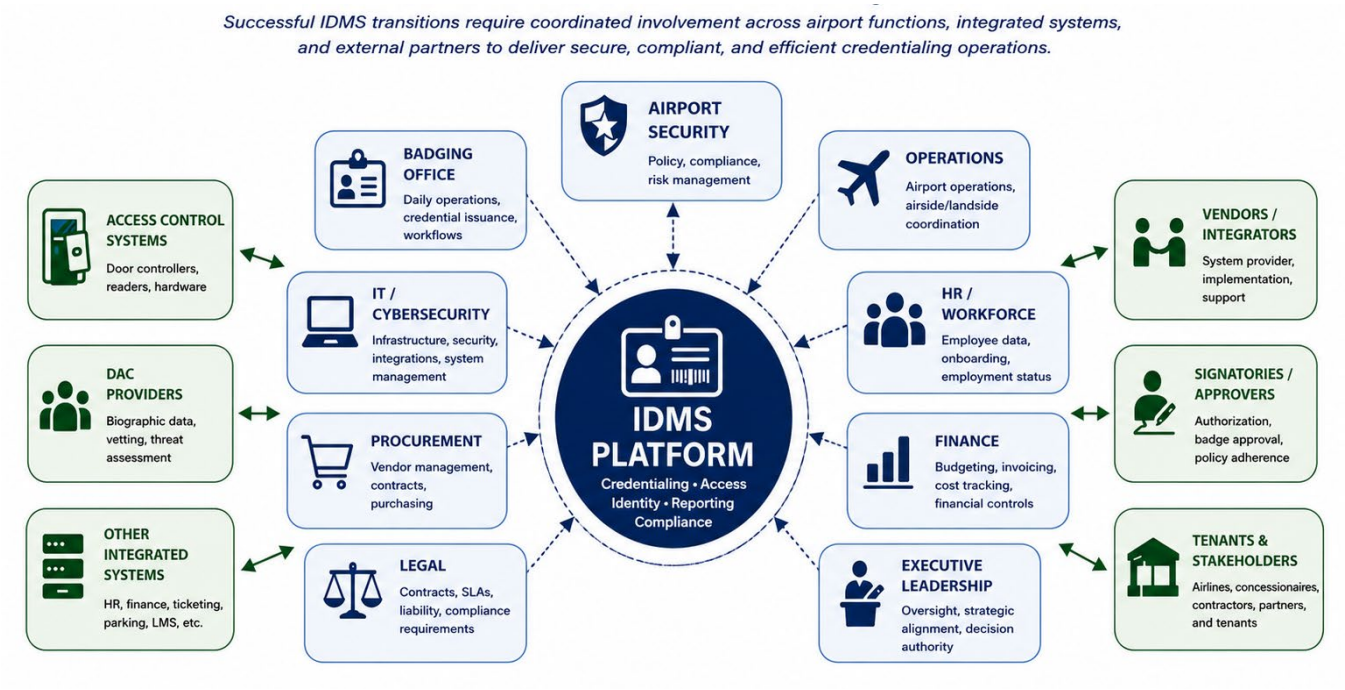
Figure 1. Modern IDMS Transition Ecosystem viii
Figure 2. Common Drivers and Operational Impacts Influencing Airport IDMS Transitions 4
Figure 3. IDMS Transition Stakeholders 9
Figure 4. Primary IDMS Requirement Categories 13
Figure 5. Common Transition Risks Identified During Airport IDMS Implementations 26
Figure 6. Key Considerations for IDMS Transition Planning 27
Figure 7. Five Pillars of Long-Term IDMS Sustainability 49

SUMMARY

This report summarizes research conducted under PARAS 0067: Guidance for Airport Identity Management System (IDMS) Transitions. The research examined how airports plan, procure, implement, and manage transitions from legacy IDMS platforms to newer operational environments. Findings were developed through interviews with airports representing multiple TSA categories, IDMS vendors, and airport personnel responsible for procurement, legal coordination, cybersecurity, operations, badging, access control, and implementation management.

Airports consistently described IDMS transitions as the result of accumulated operational, technical, cybersecurity, compliance, integration, and vendor-support challenges rather than a single system failure. Common drivers included aging infrastructure, declining vendor support, reporting limitations, manual workarounds, integration constraints, audit concerns, cybersecurity modernization needs, and evolving operational and regulatory expectations. The findings also demonstrated that modern IDMS platforms function as enterprise operational systems supporting badge holder management, credentialing workflows, access control coordination, audit readiness, reporting, compliance oversight, cybersecurity governance, and operational continuity. Figure 1 illustrates the interconnected stakeholder, system, and governance environment surrounding these transitions.

Figure 1. Modern IDMS Transition Ecosystem



The report presents practical guidance across the transition life cycle, including needs assessment, requirements development, procurement and RFP considerations, migration, integration and testing, operational continuity, cutover and go-live, cybersecurity governance, contract considerations, training, documentation, and long-term support. Across these areas, airports emphasized early stakeholder engagement, clear governance and vendor responsibilities, realistic implementation timelines, phased testing, repeated migration validation, contingency planning, and alignment between technical implementation activities and operational workflows.

Data migration, system integration, and continuity planning were frequently identified as the most complex transition workstreams. Airports stressed the need for early assessment and cleanup of legacy

records, repeated validation, realistic operational testing, phased implementation, fallback procedures, and close airport-vendor coordination. Cybersecurity considerations, including role-based access controls, multifactor authentication, vendor-access management, logging, monitoring, hosting governance, and incident response coordination should also be incorporated throughout procurement, implementation, and long-term management rather than treated as separate technical requirements.

The report captures lessons learned and provides scalable considerations for airports of varying sizes, governance structures, staffing models, and operational environments. It also identifies opportunities to update PARAS 0038 guidance related to governance, cybersecurity, migration, operational continuity, vendor accountability, implementation sequencing, and long-term lifecycle management.

PARAS ACRONYMS

ACRP	Airport Cooperative Research Program
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

ACS	Access Control System
CBP	Customs and Border Protection
CBT	Computer-Based Training
CHRC	Criminal History Records Check
CIP	Critical Infrastructure Protection
DAC	Designated Aviation Channeler
IDMS	Identity Management System
SME	Subject Matter Expert

SECTION 1: INTRODUCTION

Airport identity management systems (IDMS) play a critical role in supporting airport security, access control, regulatory compliance, credential management, and daily operational continuity. As airports continue to modernize operational and security environments, many are evaluating or replacing legacy IDMS platforms due to aging infrastructure, evolving cybersecurity expectations, operational limitations, integration challenges, and increasing compliance requirements. These transitions are often complex, involving coordination across operational, technical, procurement, legal, and regulatory stakeholders while maintaining continuity of airport operations and access control functions.

1.1 Purpose and Research Objectives

The research for this report focused on understanding why airports are replacing or upgrading their IDMS and how those transitions are being planned and implemented. Interviews with participating airports explored the operational, security, and regulatory factors driving modernization, along with practical challenges related to legacy system limitations, change management, stakeholder coordination, business process alignment, and long-term system support. This report is intended to supplement, not replace, PARAS 0038 – Airport Guidance for IDMS, by providing focused guidance on planning and implementing IDMS transitions.

To support a more comprehensive understanding of IDMS transitions, the research also includes perspectives from IDMS vendors actively involved in IDMS implementations, as well as targeted discussions with airport personnel responsible for legal and procurement functions. These additional inputs provide insight into contract structures, vendor relationships, procurement approaches, and legal considerations that influence how transitions are scoped, executed, and managed.

The objective of this research is to support informed planning and decision-making throughout an IDMS transition. The final framework is intended to provide practical, scalable considerations for airports of varying sizes, operational complexity, staffing models, and technology environments. This includes considerations related to needs assessment, system requirements, procurement, transition planning, contract management, training, and documentation.

1.2 Scope of Research

The findings summarized in this report are based primarily on interviews with airports representing multiple TSA categories that have completed or are actively undergoing IDMS transitions. Vendor interviews were conducted to supplement airport perspectives and provide broader insight into implementation practices across multiple environments. Additional discussions with airport legal and procurement stakeholders further informed findings related to contracting, risk allocation, and regulatory alignment.

Interview insights are supported by a targeted review of previous PARAS research, academic literature, and industry publications. The findings presented throughout this report reflect recurring themes and lessons identified across airport interviews, including operational drivers for transition, stakeholder coordination, cybersecurity and compliance considerations, data migration and integration challenges, operational continuity planning, vendor support expectations, and long-term life cycle management.

1.3 Research Approach and Methodology

Research activities focused primarily on structured interviews with airports that had completed or were actively engaged in IDMS transitions. Interview questions were organized around key transition topics including planning and stakeholder coordination, procurement, data migration, system integration, cybersecurity and compliance, operational continuity, training, vendor support, and long-term system management. Sample interview questions used throughout the research process are included in Appendices A through C.

Additional interviews were conducted with IDMS vendors to better understand implementation approaches, recurring airport challenges, technical considerations, and industry trends associated with IDMS modernization efforts. Discussions with airport legal and procurement stakeholders provided additional insight into contracting approaches, vendor accountability, cybersecurity considerations, and risk management practices associated with IDMS transitions.

The research also included a review of relevant PARAS reports, industry guidance, regulatory considerations, and related publications to support analysis of interview findings and identify recurring themes across multiple airport environments. Findings were evaluated collectively to identify common transition drivers, implementation considerations, operational challenges, and recurring lessons learned observed across participating airports.

1.4 Airport and Stakeholder Participation

Research participation included airports representing multiple TSA categories and varying operational environments, including differences in airport size, governance structures, staffing models, technology environments, and operational complexity. Participating airports included organizations that had recently completed IDMS transitions, were actively implementing new systems, or were in advanced planning stages for future transitions.

Participation also included IDMS vendors, airport IT personnel, security and badging representatives, procurement personnel, legal stakeholders, operations representatives, and access control administrators involved in planning, implementing, supporting, or managing IDMS environments. This range provided operational, technical, procurement, cybersecurity, and compliance perspectives across multiple phases of the transition life cycle.

SECTION 2: OVERVIEW OF IDMS TRANSITIONS

Airports participating in this research consistently described IDMS transitions as complex operational initiatives involving far more than replacement of a single software platform. Across airport environments, transitions were influenced by evolving operational, technical, cybersecurity, compliance, and organizational considerations. While each airport approached transition planning differently based on operational size, staffing models, technology environments, and organizational structure, several recurring themes and transition drivers emerged consistently throughout the interview process.

2.1 Role of IDMS in Airport Operations and Security

IDMS support a wide range of operational, security, and regulatory functions within the airport environment. Across participating airports, IDMS platforms were consistently described as critical systems supporting badge issuance, access control coordination, vetting processes, training verification, audit management, credential life cycle management, and regulatory compliance activities. In practice, these systems serve as a central operational platform connecting airport badging operations with access control systems (ACS), Designated Aviation Channelers (DAC), training systems, and other operational or security-related technologies.

Airports referenced the need for systems capable of supporting audit requirements, reporting functions, role-based access controls, data validation, automated notifications, and integration with the broader airport cybersecurity environment.

Airport interviews demonstrated that IDMS platforms are closely integrated into daily airport operations and are relied upon by multiple internal and external stakeholders, including badging offices, airport security departments, information technology personnel, operations teams, law enforcement, procurement personnel, legal departments, authorized signatories, tenants, airlines, and vendors supporting implementation and ongoing system management. Several airports also identified coordination with federal stakeholders, including TSA and Customs and Border Protection (CBP), as part of the operational and compliance environment surrounding IDMS management and transition activities.

Airport interviews also demonstrated that IDMS environments are highly interconnected with other operational systems and business processes via integrations with access control systems, DAC providers, training systems, financial systems, notification systems, or operational workflow tools. As a result, IDMS transitions often extend beyond simple software replacement efforts and require coordination across multiple technical environments, operational processes, and stakeholder groups.

In addition to supporting operational workflows, airports described IDMS platforms as increasingly important from a cybersecurity and compliance perspective. Several airports specifically identified IDMS platforms as critical systems within cybersecurity planning efforts because of their role in access management, credentialing, and operational continuity.

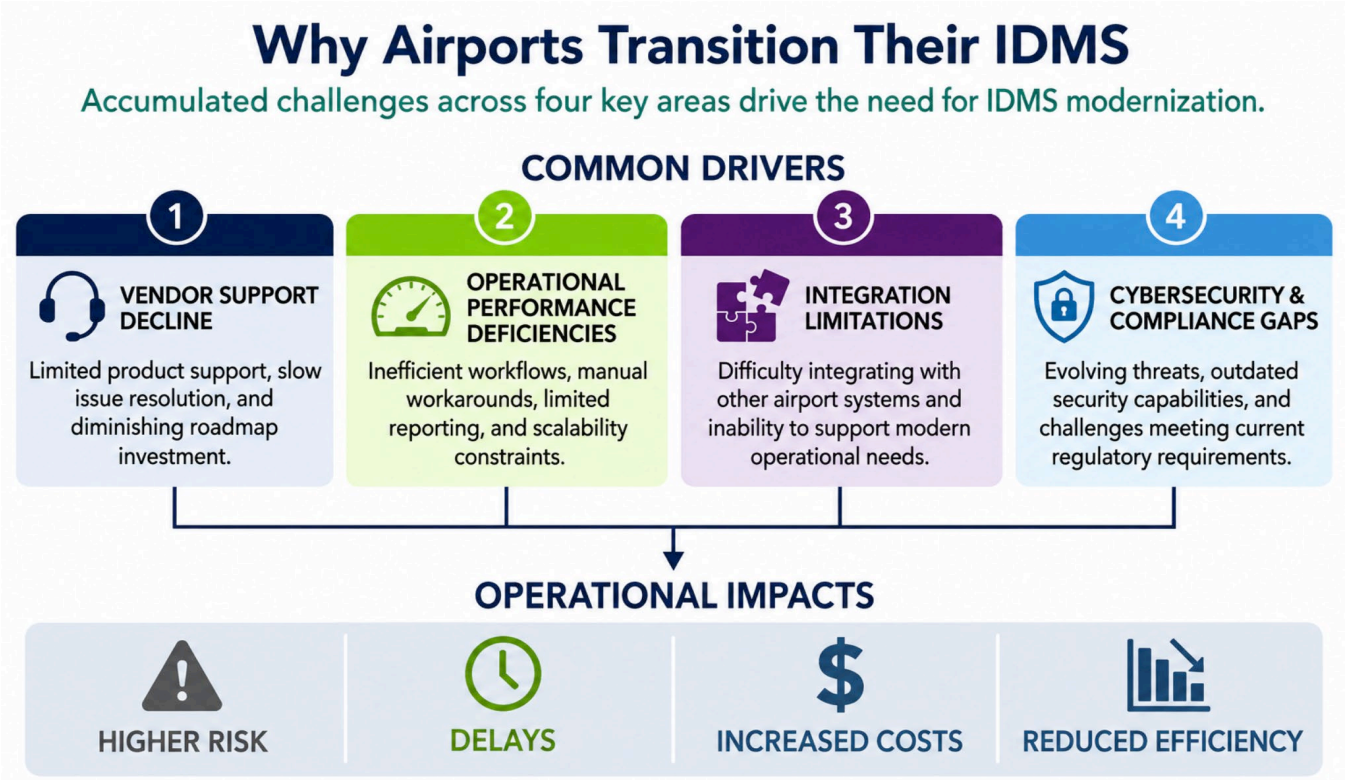
2.2 Common Drivers for IDMS Transition

IDMS transitions are rarely triggered by a solitary software bug or an isolated system failure. Modernization becomes necessary due to a gradual buildup of accumulated technical, operational, compliance, and vendor support challenges. These foundational drivers were reported primarily as four industry-wide trends:

- **Declining Vendor Support:** Legacy platforms reaching end-of-life status, characterized by unresolved technical errors, delayed support response times, and limited patch maintenance.
- **Operational Performance Deficiencies:** Core platform instabilities affecting baseline utilities like badge printing, reporting agility, data integrity, and fingerprint capture, which forces an ongoing reliance on manual workarounds.
- **Integration Limitations:** Fragmented information exchanges between legacy IDMS environments and vital supporting technologies like ACS and DAC.
- **Cybersecurity and Regulatory Gaps:** Inability of aging architectures to adapt to shifting TSA requirements, modern data encryption standards, or internal IT governance mandates like multi-factor authentication.

While these categories represent the primary strategic motivations for system modernization, Figure 2 summarizes the recurring operational and technical pressures influencing airport IDMS modernization efforts. Executing a successful transition ultimately requires translating these high-level trends into a detailed, site-specific evaluation. A comprehensive technical breakdown of these drivers, along with a structured framework for conducting current-state gap analyses and establishing a formal business justification, is detailed in Section 3: Needs Assessment.

Figure 2. Common Drivers and Operational Impacts Influencing Airport IDMS Transitions



2.3 Industry Trends and Modernization

Several recurring trends influenced how airports approached IDMS modernization efforts, including cybersecurity and compliance alignment, modern architecture considerations, vendor responsiveness, integration, and long-term life cycle management. One consistent trend involved the movement toward more integrated, automated, and operationally connected IDMS environments. Airports increasingly

described the need for platforms capable of supporting integration across multiple operational systems while reducing manual processes and improving data consistency across operational workflows.

Several trends influence how airports approach IDMS modernization efforts:

- Integration across multiple operational systems
- Reducing manual processes and improving data consistency
- Cybersecurity and compliance alignment
- Modern system architecture (with caveats)
- Vendor responsiveness and long-term support capabilities
- Long-term life cycle management

Another trend involved growing emphasis on cybersecurity and compliance alignment during system evaluation and procurement activities. Airports described incorporating cybersecurity requirements, compliance expectations, vendor security practices, and operational risk considerations earlier in the transition process than in previous system implementations. Several airports noted that cybersecurity and compliance expectations directly influenced procurement requirements, hosting decisions, implementation sequencing, and vendor evaluation activities.

Airports also described increasing interest in more modern system architectures, including cloud-based solutions and web-based operational environments. Some airports viewed cloud-based platforms as opportunities to improve flexibility, centralized management, and system maintenance capabilities, while others emphasized the need to carefully evaluate security controls, data management practices, hosting considerations, and cybersecurity requirements before implementation. However, some airports have expressed a preference for on-premises solutions due to airport-specific policy restrictions.

Vendor responsiveness and long-term support capabilities also emerged as increasingly important evaluation factors. Interviewees underscored the importance of ongoing vendor engagement, implementation support, issue resolution responsiveness, operational understanding, and long-term partnership expectations. Several airports contrasted previous experiences involving reactive or limited vendor support with newer environments emphasizing collaboration, rapid response, proactive communication, and operational alignment.

There was also increasing recognition that IDMS transitions are operational and organizational initiatives rather than solely technical implementations. Airports described the importance of stakeholder coordination, continuity planning, communication strategies, training, governance, and long-term life cycle management as major components of successful transition efforts. These trends illustrate how airports increasingly view IDMS platforms as enterprise operational systems requiring coordination across security, operations, IT, procurement, compliance, and governance functions.

SECTION 3: NEEDS ASSESSMENT

This section translates the high-level transition drivers identified in Section 2 into a structured needs-assessment process. It focuses on documenting the conditions prompting transition, engaging the stakeholders needed to define requirements, evaluating the current-state environment and gaps, and developing a business case for airport leadership and procurement. The depth and formality of the assessment should be scaled to the airport's size, governance structure, staffing model, operational complexity, and technology environment.

3.1 Current-State Evaluation and Gap Analysis

Section 2.2 identifies four recurring drivers for IDMS transition: declining vendor support, operational performance deficiencies, integration limitations, and cybersecurity and compliance gaps. During the needs assessment process, airports should translate these broad drivers into site-specific evidence, operational impacts, risks, and future-state requirements. The assessment should document both current deficiencies and the consequences of maintaining the status quo. Table 1 outlines each potential transition driver and its associated evidence to be documented for both the current system and the needs assessment.

Table 1. Documenting Evidence of Transition Needs

Transition Driver	Current-State Indicators to Document	Needs-Assessment Implications
Declining vendor support	End-of-life or limited product support; unresolved support tickets; recurring system failures; aging infrastructure; browser or equipment limitations; limited vendor responsiveness or roadmap investment	Evaluate life cycle and supportability risk and define future requirements for maintenance, escalation, issue resolution, vendor responsiveness, and post-implementation support
Operational performance deficiencies	Badge printing, fingerprint capture, reporting, reliability, or usability issues; inefficient workflows; manual workarounds; automation gaps; extended processing or ticket-resolution delays; increased administrative burden	Establish a baseline for current performance and define future requirements related to reliability, usability, reporting, automation, workflow efficiency, and operational flexibility
Integration limitations	Fragmented exchanges between the IDMS, access control system, DAC, training system, and other supporting technologies; synchronization issues; manual reconciliation; unsupported or poorly documented interfaces	Inventory existing integrations and dependencies and define future requirements for data exchange, interface reliability, synchronization, testing, migration, and cross-system coordination
Cybersecurity and compliance gaps	Audit and reporting limitations; data-accuracy concerns; outdated security capabilities; difficulty meeting TSA or airport cybersecurity requirements; challenges involving RapBack, signatory information, access controls, or operational traceability	Define cybersecurity, audit, compliance, access control, data governance, logging, monitoring, and future-proofing requirements for the replacement environment

A current-state evaluation converts the drivers discussed above into a documented baseline of the airport's existing IDMS environment. The evaluation should address operational workflows, badge issuance processes, data quality, reporting and audit capabilities, integration dependencies, compliance

and cybersecurity requirements, equipment and browser dependencies, system reliability, and vendor-support conditions. Airports described using both formal gap analyses and internal reviews, with the scope of the effort varying based on airport size, staffing capacity, governance structure, and operational complexity. Common challenges and future-state goals identified during these evaluations are summarized in Table 2.

Table 2. Common Challenges and Goals Associated with IDMS Transitions

Challenges Driving IDMS Transitions	Airport Goals for IDMS Transitions
• Reporting capabilities • Audit support • Integration challenges • Operational inefficiencies • Manual workarounds • Equipment failures • Browser dependencies • Data quality and management • Inconsistent system performance • Aging infrastructure • Inreasing administrative burden • Declining vendor responsiveness	• Stronger reporting tools • Modern system architecture (cloud-based environments) • Improved automation • Enhanced audit functionality • Improved operational visibility • Integration with other airport operational systems • Improved usability • Operational resilience and scalability • Cybersecurity requirements • Better vendor support

Operational experience should directly shape requirements development. Airports cited recurring outages, unresolved support tickets, inconsistent performance, aging infrastructure, browser and equipment limitations, automation gaps, and the administrative burden created by manual processes and data reconciliation. These conditions should be documented in terms of their effects on badging operations, user workload, compliance support, and transition planning.

Data quality and legacy system cleanup also emerged as important planning considerations during current-state evaluation activities. Airports described efforts to review existing badge records, reconcile data discrepancies, validate RapBack subscriptions, verify signatory information, and identify outdated or unnecessary records prior to migration activities. Several airports emphasized that early evaluation of legacy data conditions significantly improved migration planning and reduced downstream implementation challenges. Additional airport interviews also highlighted the operational importance of identifying duplicate records, inactive badge holders, outdated access privileges, and inconsistent data structures prior to migration activities to reduce post-implementation corrections and operational disruption.

Airports also evaluated future operational and technical needs during the assessment process. Several airports identified interest in improved automation, stronger reporting capabilities, cloud-based environments, better integration support, enhanced audit functionality, improved operational visibility, and more responsive vendor support as part of future-state planning activities. Airports also described increasing emphasis on cybersecurity requirements, operational resilience, scalability, and integration with other airport operational systems during requirements development discussions. These desired outcomes should be documented as measurable requirements rather than treated only as general modernization goals.

Several airports used the IDMS transition as an opportunity to improve related operational processes, supporting technologies, and badging office practices rather than limiting the project to replacement of

the core IDMS platform. Interviewees described updates that included adding badge icons, redesigning badge layouts using vendor-provided badge templates, updating card technology and biometric encoding formats, refreshing computers and workstations, adding or replacing ID scanners and badge readers, and changing numbering conventions by shortening or revising airport identification numbers. Some airports also identified related future improvements involving access control system coordination, training systems, and hardware refresh activities. These examples suggest that current-state evaluation activities should consider whether the IDMS transition creates an opportunity to improve adjacent processes, physical workspace needs, credential design, equipment compatibility, training workflows, and supporting system integrations before procurement and implementation decisions are finalized.

Requirements development activities frequently influenced procurement planning and vendor evaluation criteria. Airports described using operational findings, technical limitations, stakeholder input, and compliance concerns identified during current-state evaluations to support RFP development and vendor-selection activities. In several cases, airports noted that requirements became more clearly defined after operational stakeholders, IT personnel, badging offices, procurement teams, and vendor representatives participated in planning discussions and identified operational or technical dependencies that required additional consideration prior to implementation.

Vendor interviews similarly emphasized the importance of structured assessments and early data gathering before procurement and implementation activities begin. Vendors noted that airports with clearly documented operational requirements, better understanding of integration dependencies, and more realistic assessments of legacy data conditions were generally better positioned to support implementation planning, reduce scope changes, and improve overall transition coordination.

Successful IDMS transitions require more than replacement of existing technology platforms. Early operational assessments, structured requirements development, and comprehensive evaluation of legacy environments help airports better define transition objectives, align procurement activities with operational needs, anticipate implementation challenges, and support more effective coordination.

To support these activities, Appendix D provides a Current-State Evaluation Checklist that airports may use to assess existing IDMS capabilities, operational processes, reporting functionality, system integrations, data quality, compliance considerations, and other factors that may influence transition planning and requirements development.

At the conclusion of the current-state evaluation, airports should be able to answer:

- Why is the current IDMS no longer meeting operational needs?
- What operational, technical, and compliance gaps exist?
- What data cleanup activities are required before migration?
- What integrations must be maintained or improved?
- What future-state capabilities are required?
- What organizational and stakeholder impacts must be addressed?
- What procurement requirements should be included in an RFP?
- What implementation risks should be anticipated and mitigated?

Formal gap analyses, internal reviews, and development of a concept of operations can help align current-state findings, future-state workflows, stakeholder responsibilities, and implementation priorities before procurement begins. Airports that documented these conditions early were generally better positioned to develop clearer requirements and more realistic implementation sequencing. Airports

responding only after a critical failure or sudden compliance pressure often faced compressed timelines, greater operational urgency, and reduced flexibility during transition activities.

3.2 Stakeholder Identification

IDMS transitions are most effective when approached as organization-wide operational initiatives rather than isolated technology projects. Airports that establish clear governance structures, engage stakeholders and identify their roles and responsibilities early, and maintain consistent cross-functional coordination were generally more successful in managing the complex transition process.

Early stakeholder coordination and clearly defined governance structures support more effective transition planning and implementation. Airport interviews consistently identified stakeholder coordination as a major component of successful IDMS transition efforts. Airports described involvement from a wide range of internal and external stakeholders throughout planning, procurement, implementation, testing, operational transition, and long-term system management activities. While stakeholder structures varied across airport environments, recurring participants commonly included airport security personnel, badging offices, information technology departments, operations teams, procurement personnel, legal departments, access control administrators, law enforcement representatives, authorized signatories, tenants, airlines, and vendor implementation teams. These stakeholder groups are summarized in Figure 3.

Figure 3. IDMS Transition Stakeholders



IT STAKEHOLDERS

IT stakeholders help manage cybersecurity, digital infrastructure, and integration with the broader airport technology environment.

Several airports described information technology departments as playing a particularly significant role in transition planning due to cybersecurity requirements, infrastructure considerations, integration planning, hosting decisions, and coordination with broader airport technology environments. Airports frequently referenced coordination between security and IT stakeholders when evaluating system architecture, vendor access controls, cybersecurity requirements, hosting environments, and operational continuity considerations. Several airports also noted that coordination with IT became increasingly important as airports evaluated cloud-based environments, network segmentation requirements, access management controls, and cybersecurity governance expectations associated with modern IDMS platforms.

OPERATIONAL STAKEHOLDERS

Operational stakeholders ensure that operational workflows and processes are reflected within planning activities. Operational stakeholders are also heavily involved in defining transition requirements and implementation priorities. Airports described coordination with badging personnel, operations teams, access control administrators, communications centers, and tenant representatives to ensure that operational workflows, access requirements, credentialing processes, and reporting needs were reflected within planning activities. Several airports also identified law enforcement, TSA, and CBP participation as important components of stakeholder coordination depending on airport operational structure and compliance requirements.

Several airports emphasized the importance of involving operational users early in the planning process to identify workflow dependencies, operational constraints, and implementation impacts before procurement and configuration activities begin. Airports noted that operational personnel often identified practical workflow issues, reporting limitations, badge issuance concerns, and integration dependencies that may not have been fully recognized during initial planning discussions. Some airports also described challenges where operational impacts were identified later in implementation activities, resulting in additional configuration adjustments, testing delays, or compressed operational timelines.

PROCUREMENT AND LEGAL STAKEHOLDERS

Procurement and legal stakeholders manage contract structure, procurement sequencing, and operational accountability considerations. Procurement and legal stakeholders also influence planning and governance activities. Airports described coordination related to contract structure, procurement sequencing, vendor evaluation criteria, cybersecurity requirements, risk allocation, service-level expectations, and operational accountability considerations. In some cases, procurement approaches were influenced by airport governance structures, public procurement requirements, or organizational approval processes that required coordination across multiple internal departments. Vendor interviews similarly noted that airports with clearly defined governance structures and decision-making authority were often better positioned to support efficient implementation coordination and issue resolution.

GOVERNANCE STRUCTURES

Having an organized governance structure and decision-making authority is critical to the process. While governance structures varied significantly across participating airports, clearly defined decision-making authority and project coordination remained critical to interviewees. Several airports noted centralized governance approaches where core project teams coordinated major planning, procurement, implementation, and operational decisions across departments. Other airports described more distributed governance structures involving operational working groups, technical coordination teams, procurement oversight processes, and executive approval channels operating simultaneously.

Operational governance also plays an important role during implementation planning and transition activities. Airports described coordination related to testing schedules, cutover planning, operational continuity procedures, access management decisions, signatory coordination, training activities, and communication strategies. Interviewees consistently noted that governance structures became increasingly important during implementation phases where operational, technical, and organizational decisions often required rapid coordination across multiple stakeholder groups.

IDMS transitions are most effective when approached as organization-wide operational initiatives rather than isolated technology projects. Airports that established clear governance structures, identified stakeholder roles early, and maintained consistent cross-functional coordination were generally better positioned to manage implementation complexity, support operational continuity, address technical and compliance considerations, and respond to operational issues throughout the transition process.

3.3 Business Case Development

Business case development should translate current-state findings into a clear comparison between the cost and risk of maintaining the legacy environment and the investment required for transition. Where possible, airports should quantify staff time and operational impacts associated with manual workarounds, duplicate data entry, reconciliation, troubleshooting, vendor coordination, reporting limitations, recurring system failures, and other conditions that reduce productivity or increase compliance and operational risk.

Airports also emphasized that transition planning required significant staff investment across multiple stakeholder groups, including badging and security offices, IT, procurement, legal, finance, tenant organizations, and other operational partners. Activities such as workflow reviews, data cleanup and validation, assisting in requirements development, procurement support, system testing, training, issue tracking and resolution, and post-implementation stabilization represented meaningful costs that needed to be considered during business case development. However, several airports described evaluating these transition-related resource commitments against the ongoing staff time required to support legacy IDMS environments. Airports noted that recurring efforts associated with manual workarounds, data reconciliation, troubleshooting, vendor coordination, reporting limitations, duplicate processes, and continued support of aging systems consumed substantial staff resources over time. While the scope and complexity of these activities varied based on airport size and operational complexity, airports generally viewed the concentrated effort required for transition as preferable to the continuing operational burden and escalating resource demands associated with maintaining legacy platforms.

Life cycle, compliance, cybersecurity, and operational risk considerations should be evaluated together. Airports described unsupported software components, obsolete hardware, browser constraints, diminished vendor expertise, audit and reporting limitations, data accuracy concerns, and difficulty implementing current security practices as risks of continued reliance on legacy platforms. These conditions can increase the likelihood of outages, extend recovery times, create compliance exposure, and generate unexpected replacement or remediation costs.

Cost exposure was another factor influencing business case development. While modernization initiatives require upfront investment, airports frequently observed that the apparent cost savings associated with deferring transition often masked growing operational expenses. Ongoing expenditures associated with maintaining aging infrastructure, replacing obsolete equipment, supporting custom workarounds, resolving recurring technical issues, and dedicating staff time to inefficient processes can accumulate significantly over time. Several airports described evaluating not only direct procurement and implementation costs but also the long-term financial implications of continued reliance on legacy systems, including operational inefficiencies, increased support requirements, potential compliance remediation activities, and business disruption associated with system failures.

Operational scalability and modernization objectives further influenced transition justification. Airports described interest in improving usability, strengthening reporting capabilities, modernizing workflows, improving automation, supporting cloud-based environments, enhancing operational visibility, and improving integration support with other airport systems. Several airports also identified opportunities to improve operational efficiency, reduce manual processing requirements, streamline workflows, and improve long-term operational support through implementation of newer IDMS platforms. For many airports, modernization was viewed not only as a technology replacement effort but also as an opportunity to establish a more scalable, supportable, and resilient platform capable of accommodating future operational growth, regulatory changes, and evolving security requirements.

In several cases, airports also described formal or informal assessment activities used to support transition justification and planning efforts. These activities included operational reviews, gap analyses, stakeholder discussions, current-state evaluations, risk assessments, and documentation of recurring operational issues affecting implementation planning and procurement activities. Vendor interviews similarly emphasized that airports conducting structured assessments and documenting operational impacts early in the process were generally better positioned to support requirements development, procurement alignment, implementation planning, and long-term operational coordination.

The business case should present both implementation costs and status-quo risks, including resource needs, operational impacts, expected costs, risk-reduction benefits, and long-term return on investment. It should translate the transition drivers and gap-analysis findings described in Section 3.1 into a clear decision path for airport leadership and procurement. Airports that documented operational impacts early and aligned modernization with broader operational, security, and organizational objectives were generally better positioned to support stakeholder alignment and implementation success.

SECTION 4: SYSTEM REQUIREMENTS

System requirements identified throughout the research extended beyond basic credentialing functionality and reflected broader operational, technical, cybersecurity, integration, compliance, and life cycle management considerations associated with modern airport IDMS environments. Airports characterized the importance of aligning system requirements with operational workflows, implementation objectives, cybersecurity expectations, regulatory obligations, integration dependencies, and long-term operational sustainability. To help organize these findings, Figure 4 summarizes the primary functional, technical, compliance, and performance requirement categories identified through stakeholder interviews and requirements-development activities.

Figure 4. Primary IDMS Requirement Categories



Several airports emphasized that requirements development activities were heavily influenced by operational frustrations and limitations experienced within legacy environments. Common issues identified during interviews included reporting limitations, manual workflows, integration challenges, inconsistent data management, operational inefficiencies, limited automation, browser dependencies, vendor-support concerns, and difficulty adapting legacy platforms to evolving operational and compliance requirements. These operational experiences frequently shaped both procurement priorities and implementation planning activities.

The research also indicated that airports increasingly expect IDMS platforms to function as integrated operational systems rather than isolated badging applications. As a result, the need for scalable architectures, stronger integration, improved operational visibility, enhanced cybersecurity protections, better reporting functionality, more flexible workflow management, and long-term vendor support capabilities within future-state environments were identified as paramount.

4.1 Functional Requirements

Functional requirements were consistently influenced by operational workflows, badge holder management activities, signatory coordination, reporting needs, automation objectives, and broader operational efficiency goals. Airports frequently identified the need for systems that support more streamlined workflows, improved usability, enhanced reporting functionality, and reduced reliance on manual processes during day-to-day operations.

Several airports described operational frustrations associated with legacy systems that required users to navigate multiple interfaces, perform repetitive manual actions, or rely on inconsistent workflows to complete routine credentialing tasks. Other airports noted that automation gaps increased administrative workload and created inefficiencies affecting badging personnel, signatories, and operational stakeholders. Airports also described situations where limitations within legacy environments affected reporting efficiency, operational visibility, and overall workflow flexibility.

Functional Requirements:

- Reporting capabilities
- Automation of workflows and approvals
- Operational visibility and communication
- Badgeholder management

Reporting functionality was repeatedly identified as a major operational requirement. Airports emphasized the importance of accurate reporting capabilities supporting badge holder accountability, audit readiness, access management, compliance monitoring, operational oversight, and decision-making activities. Several airports also described the need for customizable reporting structures, automated notifications, dashboard functionality, and improved operational visibility to better support daily management activities and long-term oversight responsibilities.

Workflow management and signatory coordination also emerged as recurring operational considerations. Airports described the importance of supporting badge issuance workflows, fingerprint processing, training coordination, signatory approvals, access provisioning, renewal activities, and operational communication within a more integrated and user-friendly environment. Several airports also emphasized the value of systems designed specifically for airport badging environments rather than more generalized identity management platforms.

Additional airport interviews further highlighted the operational benefits associated with improved automation, step-by-step workflow structures, modernized user interfaces, and integrated dashboard functionality. Some airports specifically noted reductions in processing time, improved workflow consistency, and decreased front-desk workload following implementation of newer IDMS platforms with stronger automation and operational-management capabilities.

Functional requirements should be closely aligned with operational workflows, user experience considerations, reporting needs, automation objectives, and long-term operational management activities. Airports that incorporated operational-user input and workflow analysis early in requirements development were generally better positioned to support more effective implementation outcomes and long-term operational efficiency improvements.

4.2 Technical Requirements

Technical Requirements:

- Integration support
- Hosting environment and system architecture
- Data migration planning
- Cybersecurity coordination

Technical requirements were consistently shaped by integration complexity, infrastructure considerations, cybersecurity expectations, hosting environments, operational continuity requirements, and the need to support long-term scalability within increasingly interconnected airport technology environments. Airports frequently described legacy technical limitations as significant drivers influencing both transition planning and future-state system requirements.

Several airports identified integration support as one of the most important technical considerations during requirements development activities. Airports described dependencies involving access control systems, DAC providers, training systems, financial systems, notification platforms, visitor management

systems, and other operational technologies that required reliable communication and synchronization with the IDMS environment. In several cases, airports noted that legacy systems created fragmented workflows, inconsistent data exchange, or manual reconciliation requirements due to limited interoperability between systems.

Integration complexity also increased as airports maintained multiple systems during transition activities. Some airports described situations where maintaining multiple ACS environments or supporting legacy integrations during phased implementations significantly complicated technical coordination and testing efforts. Other airports described the need for custom interfaces, middleware solutions, or API integrations to support operational requirements not fully addressed within the core IDMS platform. Additional airport interviews also highlighted the importance of validating synchronization timing, interface reliability, API functionality, and operational dependencies prior to production deployment activities.

Environment management and infrastructure coordination emerged as major technical considerations. For example, the use of development, testing, pre-production, and production environments throughout migration, integration, and implementation activities were reported as important. These environments supported data validation, workflow testing, issue identification, operational simulation, and production-readiness assessments before go-live activities occurred. Several airports emphasized that test environments frequently required substantial coordination between vendors, IT personnel, operational stakeholders, and integration providers to ensure realistic operational validation prior to deployment.

Hosting environments and architecture decisions also influenced technical requirements discussions. Airports described evaluating cloud-hosted systems, on-premises environments, hybrid architectures, browser compatibility considerations, remote-access capabilities, infrastructure ownership responsibilities, and operational support requirements during planning and procurement activities. Several airports also referenced modernization objectives involving web-based platforms, improved browser compatibility, scalable architectures, and more flexible operational management capabilities compared to legacy environments.

Data migration and synchronization requirements further influenced technical planning activities. Airports described pulling information from multiple operational systems, reconciling inconsistent data formats, validating historical records, and coordinating synchronization activities across operational platforms during implementation efforts. Interviewees reported that legacy data conditions, undocumented workflows, inconsistent field structures, and historical operational workarounds significantly increased technical complexity during migration and integration activities.

Cybersecurity coordination also became increasingly integrated into technical requirements discussions. Airports described requirements involving role-based access controls, multifactor authentication, network segmentation, vendor-access management, access logging, system monitoring, and broader alignment with airport cybersecurity governance structures. Several airports also emphasized the importance of clearly defining infrastructure responsibilities, hosting controls, patch management expectations, and operational security procedures.

Vendor interviews similarly emphasized that technical complexity is often underestimated during early planning activities. Vendors noted that integration dependencies, infrastructure coordination, legacy data conditions, environment management, cybersecurity governance, and operational sequencing frequently become major implementation challenges requiring ongoing coordination throughout the project lifecycle. Vendors also emphasized that airports with stronger technical planning processes and clearer understanding of operational dependencies were generally better positioned to support smoother implementation activities and long-term stability.

Technical requirements should address far more than core software functionality. Integration support, infrastructure planning, environment management, cybersecurity coordination, migration planning, scalability, and long-term operational support capabilities all play major roles in determining the effectiveness and sustainability of modern airport IDMS environments.

4.3 Regulatory and Compliance Requirements

Regulatory and compliance requirements consistently influenced IDMS transition planning, procurement activities, implementation sequencing, workflows, and long-term system management expectations. Airports described the need to maintain alignment with TSA requirements, badge holder accountability processes, audit expectations, Criminal History Records Check (CHRC) procedures, and operational reporting obligations.

Regulatory Requirements:

- Alignment with TSA requirements and reporting obligations
- Audit readiness and reporting
- Maintaining accurate badgeholder records and credential management processes
- Cybersecurity governance

Several airports identified compliance management limitations within legacy environments as a major factor influencing modernization efforts and future-state requirements development. Airports described concerns involving reporting limitations, audit reliability, data accuracy, access-management inconsistencies, signatory accountability, and difficulties maintaining accurate credentialing information within older systems. Some airports also described situations where operational and system management concerns resulted in additional audit scrutiny or increased compliance-review activities.

Audit readiness and reporting functionality were repeatedly identified as significant operational requirements. Airports emphasized the importance of supporting badge audits, maintaining accurate operational records, validating badge holder information, supporting access control accountability, and preserving operational traceability throughout implementation and ongoing operations. Several airports also described the need for stronger reporting capabilities, automated notifications, improved dashboard visibility, and more efficient audit support tools within future-state environments.

Badge holder accountability and credential management processes also emerged as recurring compliance considerations. Airports described the importance of maintaining accurate badge holder records, validating active badge status, reconciling access privileges, maintaining signatory accountability, and supporting reliable CHRC and RapBack management activities throughout migration and operational processes. Additional airport interviews also highlighted the importance of reviewing historical records, identifying inactive badge holders, validating access permissions, and reconciling data discrepancies before migration activities occurred.

Regulatory alignment also influenced operational planning and implementation sequencing. Airports described the need to coordinate badge issuance processes, training activities, operational workflows, and access management functions in ways that maintained regulatory compliance. Several airports emphasized that maintaining operational continuity while preserving compliance obligations required substantial coordination between airport security personnel, operational stakeholders, IT departments, vendors, and external agencies.

Cybersecurity governance increasingly overlapped with regulatory and compliance expectations during planning and implementation activities. Airports described requirements involving role-based access controls, multifactor authentication, access logging, system monitoring, vendor-access management, network segmentation, and broader alignment with airport cybersecurity governance structures. Several

airports also emphasized the importance of clearly defining operational accountability, vendor responsibilities, incident response expectations, and hosting security requirements during procurement and implementation planning activities.

Vendor interviews similarly emphasized that compliance expectations have become increasingly integrated into operational and technical implementation activities within modern IDMS environments. Vendors noted that airports are placing greater emphasis on audit functionality, traceability, access accountability, cybersecurity governance, reporting reliability, and oversight capabilities throughout procurement and implementation activities compared to earlier implementation environments.

Taken together, the findings demonstrate that regulatory and compliance requirements should be integrated throughout the full IDMS transition life cycle rather than addressed as isolated operational tasks. Early coordination between operational stakeholders, IT personnel, cybersecurity teams, procurement departments, vendors, and regulatory partners helps support stronger operational accountability, improved audit readiness, more reliable compliance management, and more effective long-term operational governance within modern airport IDMS environments.

4.4 Performance Requirements

Performance requirements consistently influenced airport expectations related to operational reliability, implementation stability, reporting efficiency, workflow management, vendor responsiveness, and long-term system sustainability. Airports frequently described operational performance limitations within legacy environments as major drivers supporting modernization efforts and future-state requirements development.

Performance Requirements:

- Reliability and continuity
- Improved automations and streamlined workflows
- Reduced manual processing
- Vendor responsiveness and support
- Scalability and long-term functionality

Several airports described recurring operational issues involving system instability, delayed processing, unresolved support tickets, browser limitations, equipment failures, inconsistent synchronization, reporting inefficiencies, and broader workflow disruptions affecting daily credentialing activities. Airports also described situations where users adapted to recurring workarounds, inefficient workflows, and inconsistent system functionality for extended periods before overall impacts made transition efforts unavoidable.

Reliability and continuity were repeatedly identified as major performance considerations. Airports emphasized the importance of stable environments supporting badge issuance, fingerprint processing, access provisioning, reporting functions, operational visibility, and integration reliability. Several airports also described the importance of minimizing downtime and maintaining continuity during migration, testing, cutover, and post-implementation stabilization activities.

Processing efficiency and workflow performance also emerged as recurring priorities. Airports described the operational value of improved automation, more streamlined workflows, reduced manual processing requirements, improved dashboard visibility, and enhanced reporting functionality within newer IDMS environments. Some airports specifically reported reductions in processing time, improved front-desk efficiency, stronger workflow consistency, and improved operational management capabilities following implementation of more modernized platforms.

Vendor responsiveness and support performance were also identified as major long-term operational considerations. Several airports contrasted legacy environments involving delayed issue resolution,

reactive troubleshooting approaches, inconsistent communication, and limited support with newer support models emphasizing proactive engagement, faster ticket resolution timelines, and more collaborative coordination. Additional airport interviews also emphasized the importance of clearly defined escalation procedures, support expectations, and identified vendor points of contact following implementation activities.

Scalability and long-term adaptability further influenced performance-related discussions. Airports described the importance of supporting future operational growth, evolving compliance requirements, increased integration demands, modernization initiatives, cybersecurity expectations, and future technology expansion within long-term system planning activities. Airports emphasized that implementation and procurement decisions made during transition activities directly affected future operational flexibility and long-term system supportability.

Testing and validation activities also played an important role in supporting operational performance objectives. Airports described conducting repeated migration testing, validation exercises, integration testing, workflow simulations, and quality control reviews across multiple environments prior to deployment. Several airports emphasized that implementation success depended heavily on validating functionality under realistic conditions before production cutover activities occurred.

Vendor interviews similarly emphasized that operational performance expectations increasingly extend beyond core software functionality. Vendors noted that airports are placing greater emphasis on implementation coordination, issue resolution responsiveness, reliability, reporting performance, integration stability, scalability, and long-term support than in previous implementation environments. Vendors also emphasized that airports with stronger governance processes, clearer operational ownership, and more structured planning activities were generally better positioned to maintain long-term operational stability and performance following implementation.

Performance requirements should address reliability, workflow efficiency, support responsiveness, scalability, implementation stability, and long-term sustainability in addition to technical system functionality. Airports that incorporated these performance considerations into requirements development and procurement planning were generally better positioned to support more stable, efficient, and sustainable IDMS environments following implementation activities.

SECTION 5: PROCUREMENT CONSIDERATIONS

Procurement planning, including the development of procurement strategies and the preparation of solicitation documents such as RFPs, task orders, requirements documents significantly influenced implementation coordination, vendor accountability, alignment, and long-term system performance throughout IDMS transition efforts.

Research on procurement practices focused on the solicitation as well as practices around contract negotiation and drafting. The result of that research is the identification of key issues occurring in negotiations and some important considerations for contract terms. The following sections summarize recurring procurement strategies, development, vendor-evaluation, and implementation-coordination considerations and contract preparation identified throughout airport, vendor, procurement, and legal stakeholder interviews.

5.1 Procurement Strategy

Procurement strategy significantly influences implementation sequencing, operational coordination, vendor accountability, and long-term system sustainability throughout IDMS transition efforts. Airports described a range of procurement approaches based on governance structures, organizational policies, timelines, implementation objectives, and airport-specific procurement requirements. These approaches included formal RFP processes, less formal task-order process through existing contracts' cooperative purchasing agreements, sole-source justifications, phased procurement activities, and contract modifications associated with existing systems or technology environments.

According to interviewees, procurement activities should be approached as operational planning functions rather than solely purchasing exercises. Airports frequently described the importance of incorporating workflows, implementation sequencing, integration dependencies, cybersecurity expectations, support obligations, continuity considerations, and long-term life cycle management requirements into procurement planning activities before vendor selection efforts begin. Airports indicated that whatever approach was selected, the preparation of a detailed scope document greatly facilitated both the solicitation and contracting processes and documentation.

Key Considerations for Procurement Strategy

- Identify key stakeholders early and develop strong governance structure
- Clarify workflows, implementation sequencing, integration dependencies, cybersecurity requirements, and support expectations
- Simplify scope and reduce unnecessary customization where possible
- Begin implementation planning and operational readiness activities early
- Balance operational functionality with long-term maintenance and support
- Consider engaging an independent IDMS SME consultant or Owner's Representative to support requirements development, procurement activities, project management, implementation oversight, and vendor accountability throughout the transition life cycle

Several airports identified the benefit of engaging an independent subject matter expert (SME) consultant or Owner's Representative to support transition planning, procurement, and implementation activities. An independent consultant represents the airport's interests throughout the project and can provide objective guidance regarding requirements development, procurement strategy, stakeholder coordination, implementation planning, and project governance.

SME consultant support may include facilitating needs assessments and gap analyses, assisting with development of RFP requirements and evaluation criteria, supporting proposal reviews and vendor selection activities, advising during contract negotiations, and providing project management and

technical oversight during implementation. Airports with limited internal experience implementing IDMS solutions may find independent advisory support particularly valuable for reducing procurement risk, strengthening vendor accountability, and improving implementation outcomes.

Stakeholder coordination also played a significant role in procurement strategy development. Airports described participation from airport security personnel, IT departments, procurement teams, legal stakeholders, operations personnel, access-control administrators, executive leadership, finance departments, and vendor representatives. Several airports also emphasized that early coordination between operational, legal, and procurement personnel improved alignment between operational needs and procurement documentation during transition efforts.

Operational lessons learned from previous implementations frequently influenced procurement strategy decisions. Some airports described efforts to reduce unnecessary customization, simplify scope, strengthen accountability language, improve support expectations, and clarify implementation responsibilities based on challenges experienced within previous IDMS environments. Other airports described increasing emphasis on flexibility, scalability, operational support, cybersecurity governance, and long-term vendor responsiveness during procurement planning activities.

Procurement sequencing also emerged as an important consideration. Several airports described situations where implementation planning, infrastructure preparation, integration coordination, or operational readiness activities began prior to completion of formal procurement processes, creating compressed timelines and additional coordination challenges during later implementation phases. Other airports emphasized that early procurement alignment improved implementation coordination, planning, and vendor accountability throughout the transition life cycle.

Additional airport interviews highlighted the importance of balancing operational functionality with long-term maintainability, supportability, and life cycle management considerations during procurement planning. Several airports noted that earlier implementations attempted to address operational challenges through extensive customization efforts, resulting in increased system complexity, higher support costs, longer upgrade cycles, and greater long-term dependence on vendor-specific development. In some cases, airports reported that customizations implemented to accommodate unique local processes ultimately created operational constraints, complicated future enhancements, and made subsequent modernization efforts more difficult and costly.

Airports and vendors consistently emphasized that modern IDMS platforms are highly configurable and capable of supporting a wide range of airport operational requirements through vendor-supported settings and business rules. Configuration generally refers to using standard platform capabilities such as workflows, roles, permissions, notifications, reports, forms, data fields, approval processes, and business-rule parameters that can be modified without altering the underlying software. Many operational requirements that airports may initially perceive as requiring customization can often be addressed through thoughtful configuration, process refinement, or adjustment of legacy workflows to align with industry-standard system capabilities.

Airports also noted the value of engaging an experienced IDMS SME consultant during requirements development, procurement, and implementation planning activities. A knowledgeable SME can help airports objectively evaluate existing workflows, distinguish between operational requirements and legacy practices, and identify opportunities for business process re-engineering that support adoption of standard system capabilities. Because modern IDMS platforms are highly configurable, successful implementations often require airports to reconsider long-standing processes that may have evolved around the limitations of previous systems rather than current operational needs. An experienced SME

can facilitate stakeholder discussions, document future-state workflows, evaluate configuration options, and guide decision-making regarding when process changes are preferable to software customization. This approach helps airports maximize the use of vendor-supported configuration, reduce unnecessary customization, improve long-term maintainability and supportability, and align operational practices with industry standards and leading practices.

Vendor interviews similarly emphasized that procurement strategy significantly affects implementation coordination and long-term operational success. Vendors noted that airports with clearly defined operational objectives, realistic implementation expectations, stronger governance structures, and more structured procurement planning were generally better positioned to support smoother implementation activities and more effective long-term operational coordination.

Airports should also identify potential unplanned or underestimated cost drivers early in procurement planning. Interviewees described several transition-related costs that were not always fully apparent at the beginning of implementation, including data migration and cleanup, staff time for manual reconciliation and validation, accelerated timeline costs, multifactor authentication tokens, software licensing, fingerprint-storage licensing, additional encoding time, and office modifications to accommodate larger badge printers. Replacement of incompatible hardware such as fingerprint scanners, document-verification equipment, cameras, and related peripherals were noted as additional costs associated with transition. Some airports also noted costs or resource impacts associated with integration coordination, third-party system connections, storage needs, and hardware upgrades required to support the new IDMS environment. Identifying these items before solicitation and contract execution can help airports reduce underbudgeting risk, clarify vendor and airport responsibilities, and better align procurement documents with the full cost of implementation.

Procurement strategy should align operational requirements, technical planning, cybersecurity expectations, implementation sequencing, governance structures, and long-term support objectives early in the transition life cycle. Airports that approached procurement planning as a coordinated operational initiative rather than a standalone purchasing activity were generally better positioned to support more effective implementation outcomes and long-term system sustainability.

5.2 Solicitation Structure

Solicitation structure significantly influences vendor responses, implementation alignment, operational expectations, and long-term project coordination throughout IDMS transition efforts. Airports consistently observed the importance of developing procurement documentation that clearly defined operational objectives, technical requirements, implementation expectations, cybersecurity responsibilities, integration dependencies, support obligations, and long-term operational considerations prior to vendor selection activities. Clearly memorializing terms was important whether the solicitation took the form of an RFP, task order, or other requirements document.

Key Considerations for Solicitation Structure

- Align RFP language with operational workflows and implementation needs, in addition to technical functionality
- Ensure procurement language includes accountability expectations, implementation responsibilities, support obligations, and vendor deliverables
- Incorporate cybersecurity and compliance requirements, infrastructure ownership, and operational accountability into RFP
- Include requirements around migration planning, testing, validation, integration coordination, training, and post-implementation support
- Consider requiring vendors to coordinate with airport-retained consultants, Owner's Representatives, or independent project managers who may provide implementation oversight and validation services on behalf of the airport

Several airports described the importance of aligning solicitation language with operational workflows and real-world implementation needs rather than focusing exclusively on technical functionality. Airports frequently incorporated requirements related to operational efficiency, reporting capabilities, workflow management, badge holder accountability, integration support, cybersecurity governance, implementation coordination, training expectations, and long-term operational support within procurement documentation.

Some airports also included requirements for vendors to cooperate with airport-retained consultants or independent project managers responsible for implementation oversight. Clearly defining coordination expectations between the vendor, airport staff, and third-party advisors can improve communication, streamline issue resolution, and strengthen accountability throughout implementation. Operational lessons learned from previous implementations also influenced RFP-development activities. Some airports described revising procurement language to strengthen accountability expectations, clarify implementation responsibilities, improve support obligations, reduce excessive customization requirements, and better align vendor deliverables with operational realities identified during previous deployments. Other airports emphasized the importance of developing broader operational scopes focused on core functionality and maintainability rather than attempting to address every operational process through custom system development.

Cybersecurity and compliance expectations increasingly influenced RFP structure and procurement documentation. Airports described incorporating requirements related to role-based access controls, multifactor authentication, hosting environments, vendor-access procedures, access logging, cybersecurity governance, operational monitoring, incident-response expectations, and data protection responsibilities into procurement documentation and evaluation activities. Several airports also emphasized the importance of clearly defining infrastructure ownership, support responsibilities, operational accountability, and vendor-access limitations prior to implementation activities.

Implementation planning and operational continuity considerations were also frequently incorporated into procurement documentation. Airports described including requirements related to migration planning, testing environments, operational validation, integration coordination, cutover sequencing, training activities, stabilization support, and post-implementation operational coordination within RFP materials. Several airports identified that clearly defined implementation expectations improved vendor alignment and reduced operational uncertainty during transition activities.

Vendor-support expectations similarly played a major role in RFP-development activities. Airports described incorporating service-level expectations, escalation procedures, issue resolution timelines, operational support responsibilities, training obligations, and ongoing coordination expectations into procurement documentation to address challenges experienced within previous vendor relationships. Additional airport interviews also highlighted the operational importance of identifying dedicated support contacts, escalation paths, and implementation accountability structures within procurement documentation before contract execution.

Vendor interviews similarly emphasized that well-structured RFP documentation significantly improves implementation coordination and operational alignment. Vendors noted that airports with clearly defined operational requirements, realistic implementation expectations, stronger governance structures, and more comprehensive procurement documentation were generally better positioned to support smoother implementation activities and more effective long-term operational coordination.

Collectively, the findings demonstrate that RFP structure should support operational clarity, implementation coordination, cybersecurity governance, vendor accountability, and long-term operational sustainability throughout the IDMS transition process. Airports that developed procurement

documentation aligned with operational workflows, technical realities, implementation sequencing, and long-term support expectations were generally better positioned to support more effective vendor evaluation and implementation outcomes.

5.3 Vendor Evaluation Criteria

Vendor evaluation criteria significantly influence implementation success, operational alignment, long-term support quality, and overall system sustainability. Selection activities should extend beyond evaluation of core software functionality and include broader operational, technical, cybersecurity, implementation, and support-related considerations.

Key Considerations for Vendor Evaluation

- Align RFP language with operational workflows and implementation needs, in addition to technical functionality
- Ensure procurement language includes accountability expecations, implementation responsibilities, support obligations, and vendor deliverables
- Incorporate cybersecurity and compliance requirements, infrastructure ownership, and operational accountability into RFP
- Include requirements around migration planning, testing, validation, integration coordiation, training, and post-implementation support

Where an airport utilizes an independent SME consultant or Owner's Representative, that individual or team may also support proposal evaluations, demonstration scoring, reference checks, implementation planning reviews, and contract negotiations. Several airports noted that independent expertise helped validate vendor claims, identify implementation risks, and evaluate long-term operational impacts beyond the functionality demonstrated during procurement activities.

Several airports described operational experience and airport-specific implementation knowledge as important vendor evaluation factors. Airports frequently emphasized the value of vendors familiar with airport badging environments, TSA compliance requirements, operational workflows, integration dependencies, and credential-management processes. Some airports specifically noted that vendors with stronger operational understanding and airport-specific experience were better positioned to manage implementation coordination, operational troubleshooting, workflow alignment, and long-term support activities.

Vendor responsiveness and support quality were also repeatedly identified as major evaluation considerations. Airports described previous experiences involving delayed issue resolution, inconsistent communication, unresolved concerns, and reactive support approaches within legacy environments that significantly influenced future vendor selection priorities. Several airports emphasized the importance of evaluating responsiveness, escalation procedures, ticket-resolution timelines, support accessibility, and long-term vendor engagement during procurement and vendor selection activities.

Implementation capabilities also played a significant role in vendor evaluation activities. Airports described assessing implementation planning approaches, migration support capabilities, testing coordination processes, integration experience, training resources, readiness support, and post-go-live stabilization capabilities during vendor review activities. Additional airport interviews also highlighted the importance of evaluating vendor coordination during migration, validation, troubleshooting, and cutover activities before implementation efforts begin.

Cybersecurity posture and operational governance expectations increasingly influenced vendor-evaluation criteria. Airports described incorporating evaluation considerations related to hosting environments, access-management controls, cybersecurity governance practices, vendor-access procedures, incident-response expectations, infrastructure management responsibilities, and operational security coordination into procurement and evaluation activities. Several airports also emphasized the

importance of understanding vendor responsibilities related to monitoring, patch management, access logging, and long-term cybersecurity support before implementation begins.

Scalability, flexibility, and long-term sustainability also emerged as recurring evaluation considerations. Airports described interest in vendors capable of supporting future growth, evolving compliance requirements, additional integrations, modernization initiatives, flexibility, and future technology expansion over the life cycle of the system. Some airports also emphasized the importance of avoiding excessive customization requirements that could complicate long-term maintenance and operational support activities.

Operational usability and workflow alignment similarly influenced vendor selection activities. Airports described evaluating user-interface functionality, workflow structure, reporting capabilities, automation support, dashboard visibility, and operational efficiency improvements during demonstrations and evaluation exercises. Several airports also identified the operational value of systems designed specifically for airport badging environments with stronger workflow integration and more user-friendly operational management capabilities.

Vendor interviews similarly emphasized that successful implementations depend heavily on operational alignment and long-term coordination rather than software functionality alone. Vendors noted that airports with clearly defined objectives, realistic implementation expectations, stronger governance structures, and more comprehensive evaluation processes were generally better positioned to support more effective implementation coordination and long-term success.

5.4 Demonstrations and Proof of Concept

Demonstrations and proof-of-concept activities support operational validation, stakeholder engagement, workflow evaluation, and implementation planning throughout IDMS procurement and vendor selection efforts. Airports identified the importance of evaluating systems within the context of real-world airport operational environments rather than relying solely on written proposals or technical specifications during vendor selection activities.

Key Considerations for Demonstrations and Proof of Concept

- Focus on operational workflows, integration functionality, usability, cybersecurity coordination, and real-world implementation considerations rather than software functionality alone
- Validate integration capabilities, synchronization processes, reporting functionality, and dependency during demonstration to better understand implementation complexity and impact
- Understand cybersecurity and hosting options and the benefits and drawbacks of different systems
- Review real implementation examples, use cases, and operational scenarios

Several airports described demonstration activities that focused on operational workflows, badge holder management processes, reporting functionality, dashboard visibility, automation capabilities, integration support, signatory coordination, and overall usability. Airports commonly evaluated how systems supported day-to-day credentialing operations, access-management workflows, audit readiness activities, and operational efficiency objectives.

Operational usability consistently emerged as a significant evaluation consideration during demonstrations. Airports described frustrations within legacy environments involving complex navigation, repetitive manual actions, inconsistent workflows, reporting limitations, and inefficient operational processes that influenced evaluation priorities during vendor demonstrations. Several airports also emphasized the operational value of step-by-step workflow structures, more intuitive user

interfaces, integrated dashboard functionality, automated notifications, and systems designed specifically for airport badging operations.

Integration functionality and operational coordination were also important demonstration considerations. Airports frequently evaluated how systems interfaced with access control systems, DAC providers, training systems, notification platforms, and other technologies during vendor-review activities. Several airports observed the importance of validating integration capabilities, synchronization processes, reporting functionality, and dependencies during demonstrations to better understand implementation complexity and impacts prior to procurement decisions.

Stakeholder participation also played a significant role throughout demonstration and proof-of-concept activities. Airports described involvement from airport security personnel, badging offices, IT departments, procurement personnel, operational users, executive leadership, and vendor implementation teams during system evaluations. Operational user participation during demonstrations improved workflow evaluation, requirements validation, and long-term operational alignment.

Cybersecurity and hosting considerations increasingly influenced demonstration and proof-of-concept discussions. Airports described evaluating hosting environments, access-management controls, operational security procedures, vendor-access governance, infrastructure responsibilities, and broader cybersecurity coordination expectations during vendor-review activities. Several airports also emphasized the importance of understanding operational support models, expectations for coordinating implementation activities, and long-term vendor support models during evaluation activities.

Additional airport interviews also highlighted the value of reviewing real implementation examples, airport-specific use cases, workflow demonstrations, and operational scenarios similar to the airport's own environment during procurement activities. Some airports emphasized that practical demonstrations tied directly to operational workflows provided significantly greater value than generalized product overviews during vendor evaluations. Airports also emphasized the value of speaking directly with peer airports operating the systems under consideration, particularly those using similar access control systems, DAC providers, training platforms, hosting environments, or other major integrations. While demonstrations provide insight into product capabilities, discussions with existing airport users can provide practical information regarding implementation effort, vendor responsiveness, upgrade experience, operational impacts, and long-term supportability. Lessons learned from comparable implementations can provide perspectives that were not always apparent during demonstrations or evaluations.

Vendor interviews similarly emphasized that demonstrations and proof-of-concept activities provide important opportunities to align operational expectations, identify workflow dependencies, validate technical assumptions, and improve implementation planning before contract execution. Vendors also noted that airports with stronger stakeholder participation and more structured evaluation processes were generally better positioned to support smoother implementation coordination and operational alignment.

Demonstrations and proof-of-concept activities should focus on operational workflows, integration functionality, usability, cybersecurity coordination, and real-world implementation considerations rather than software functionality alone. Airports that incorporated operational validation and stakeholder engagement into evaluation activities were generally better positioned to support more informed procurement decisions and more effective long-term implementation outcomes.

SECTION 6: TRANSITION PROCESS

Transition activities significantly influence operational continuity, implementation stability, stakeholder coordination, and long-term IDMS performance. Airports consistently described transitions as coordinated operational initiatives involving migration planning, integration, testing, training, cutover sequencing, vendor coordination, and post-implementation stabilization.

Several airports noted that transition activities became more complex than initially anticipated due to integration dependencies, legacy data conditions, operational continuity requirements, and the need to maintain uninterrupted credentialing and access-management functions during implementation. Airports also highlighted the importance of phased planning, realistic testing, operational validation, and structured stakeholder coordination throughout implementation efforts.

Airports may benefit from engaging an independent SME consultant or Owner's Representative to provide project management support, implementation oversight, and technical guidance throughout the transition process. Airports with limited experience managing large-scale IDMS implementations may find this support particularly valuable.

Transition success was consistently influenced by early planning, realistic timelines, defined governance structures, migration readiness, technical coordination, vendor responsiveness, and the ability to balance implementation progress with ongoing operational requirements. Figure 5 summarizes common transition risks identified across airport interviews.

Figure 5. Common Transition Risks Identified During Airport IDMS Implementations

RISK AREA	WHAT THIS LOOKS LIKE	OPERATIONAL IMPACT
Data Quality & Migration	Incomplete, inaccurate, or inconsistent credential data; limited validation.	Migration delays, access errors, higher costs.
Stakeholder Coordination	Unclear roles, inconsistent communication, late engagement.	Misaligned requirements, rework, delays in decisions.
Integration Complexity	Multiple interfaces and dependencies; limited documentation.	Integration failures, workflow disruptions, extended timelines.
Testing & Validation	Insufficient end-to-end testing; limited user acceptance testing.	Issues at go-live, operational disruptions, reduced confidence.
Cybersecurity & Access Management	Gaps in vendor access controls; insufficient cybersscurity requirements.	Increased risk exposure, compliance findings, delays in approvals.
Timeline & Resources	Compressed timelines; competing priorities; limited staffing or expertise.	Project slippage, higher stress on teams and vendors, scope trade-offs.

6.1 Transition Planning

Transition planning significantly influences implementation sequencing, operational continuity, stakeholder coordination, migration readiness, and overall implementation stability throughout IDMS modernization efforts. Effective transition planning requires coordination across operational, technical,

procurement, cybersecurity, and governance activities well before implementation and cutover activities begin.

Several airports described transition planning as an operational process rather than solely a technical implementation activity. Airports frequently coordinated planning efforts across airport security departments, badging offices, IT organizations, procurement personnel, legal stakeholders, operations teams, access control administrators, executive leadership, vendor implementation teams, and external operational partners. Interviewees reported that early stakeholder engagement improved implementation sequencing and workflow coordination. It also reduced confusion later in deployment activities. Key considerations associated with IDMS transition planning are summarized in Figure 6.

Figure 6. Key Considerations for IDMS Transition Planning

Current State Evaluation	Implementation and Sequencing	Operational Governance and Continuity	Data Readiness and Integration	Vendor Coordination
Document operational frustrations, inefficiencies, and other concerns early in the process	Compressed timelines, evolving requirements, or unexpected integration dependencies increased implementation complexity.	Clearly-defined governance structures, phased planning approaches, and contingencies are critical.	Evaluate and normalize legacy data early in the process to reduce downstream issues.	Strong planning processes, clear objectives, realistic expectations, and structured governance activities can lead to a smoother implementation.

Current-state evaluations and operational assessments also played a major role in transition planning activities. Airports described conducting gap analyses, workflow reviews, operational assessments, data evaluations, integration reviews, and requirements-development discussions prior to procurement and implementation activities. Airports emphasized that documenting operational frustrations, workflow inefficiencies, integration limitations, reporting gaps, and support-related concerns early in the process improved planning coordination and helped define implementation priorities throughout transition activities.

Implementation sequencing and timeline management were also identified as recurring planning considerations. Airports described balancing procurement schedules, integration coordination, migration preparation, operational continuity requirements, testing activities, training schedules, and go-live planning throughout implementation efforts. Several airports noted that compressed timelines, delayed procurement activities, evolving operational requirements, or unexpected integration dependencies increased implementation complexity and operational risk during later project phases.

Operational governance structures also influenced transition planning effectiveness. Airports described establishing project teams, working groups, executive oversight structures, coordination processes, and stakeholder communication channels. It was noted that clearly defined governance structures improved issue resolution, implementation coordination, communication, and decision-making throughout migration and cutover activities.

Several airports noted that independent project-management or SME support can strengthen governance activities. While the IDMS vendor is responsible for delivering and configuring the system, an independent SME can help represent the airport's interests by providing dedicated oversight of implementation schedules, risk registers, issue management processes, stakeholder communications, and

vendor coordination efforts. Independent advisors can also assist airports in validating implementation plans, reviewing project deliverables, facilitating decision-making processes, and ensuring operational priorities remain appropriately represented throughout the transition life cycle.

For airports with limited internal staffing resources or limited prior experience implementing IDMS platforms, SME consultants may provide expertise related to migration planning, integration sequencing, testing strategies, operational readiness activities, and cutover preparation. This support can help reduce implementation risk and improve coordination between airport stakeholders and vendor implementation teams.

Data readiness and integration planning were similarly identified as major transition planning considerations. Airports described the importance of evaluating legacy data conditions, identifying integration dependencies, validating workflows, coordinating environment-management activities, and planning migration sequencing prior to implementation activities. Additional airport interviews also highlighted the importance of identifying duplicate records, outdated badge holder information, synchronization issues, and dependencies early in the planning process to reduce downstream implementation disruptions.

Operational continuity planning also emerged as a significant transition consideration. Airports described efforts to minimize disruptions to badge issuance, credential management activities, access provisioning, reporting functions, and workflows throughout implementation. Several airports emphasized the importance of phased planning approaches, contingency procedures, fallback processes, and readiness coordination.

Vendor coordination also played a major role during planning activities. Airports frequently described ongoing coordination with vendors related to implementation sequencing, migration planning, integration support, environment management, testing coordination, training activities, cybersecurity expectations, and post-go-live support. Vendor interviews similarly emphasized that airports with stronger planning processes, clearer objectives, realistic implementation expectations, and more structured governance activities were generally better positioned to support smoother implementation coordination and operational stability.

Interviewees described transition planning as a coordinated operational-management process involving governance, migration readiness, integration planning, continuity preparation, and long-term sequencing. Airports that established structured planning activities early in the transition life cycle were generally better positioned to support more stable implementation outcomes and reduce disruption throughout modernization efforts.

6.2 Data Migration Strategy

Data migration strategy significantly influences implementation complexity, continuity, data reliability, integration stability, and post-implementation system performance throughout IDMS transition efforts. Airports reported migration activities as one of the most complex and resource-intensive phases of implementation efforts due to legacy data conditions, integration dependencies, validation requirements, and the need to maintain continuity during transition activities.

Data migration should be treated as a major implementation workstream, not a one-time technical task. Successful migrations require early assessment of legacy data conditions, coordination across integrated systems, repeated testing and validation cycles, and active participation from multiple departments. Airports often underestimate migration complexity; data quality issues, integration dependencies, and operational continuity requirements can significantly influence implementation risk, deployment readiness, and post-implementation stability.



Several airports described migration planning as a phased and iterative process rather than a single transfer event. Airports frequently conducted multiple rounds of migration testing, validation, reconciliation, quality-control review, and exception handling activities across development, testing, pre-production, and production environments prior to final cutover activities. Several airports emphasized the importance of repeated validation activities before deployment.

Operational users, badging personnel, IT teams, vendors, and integration stakeholders were all involved in verifying migration accuracy. Airports also noted that migration activities typically involved data from multiple source systems, with the primary sources generally including the access control system, the computer-based training (CBT) system, and the DAC. Depending on the airport's operating environment, additional information may also be obtained from financial systems, human resource systems, identity providers, and other operational platforms that support credentialing and access-management processes. Ensuring consistency across these interconnected systems was frequently identified as a critical prerequisite for successful migration. Legacy data conditions also significantly influenced migration complexity. Airports described challenges involving duplicate records, outdated badge holder information, inconsistent data structures, incomplete historical records, synchronization discrepancies, inactive badge holders, signatory inconsistencies, and undocumented workarounds within legacy environments.

Interviewees stated that substantial data-cleanup was required prior to migration efforts, including reconciliation of badge holder records, validation of access privileges, review of historical information, and coordination across systems to improve migration readiness. These data migration strategy components and implementation impacts are summarized in Table 3. To support these activities, Appendix E provides a Data Migration Strategy Checklist that airports may use to evaluate legacy data conditions, source system dependencies, validation requirements, reconciliation activities, testing environments, cutover readiness, and post-migration stabilization considerations.

Table 3. Key Components of Data Migration Strategy During IDMS Implementation

Migration Focus Area	Key Considerations	Implementation Impact
Data Validation and Verification	Data clean-up, record reconciliation, duplicate removal, and data quality review	Improves migration accuracy and reduces downstream errors during deployment

Environment Management	Multiple migration cycles, accuracy verification, exception management, reconciliation reviews	Identifies issues before go-live and increases confidence in migrated data
Integration Coordination	System synchronization, cross-platform consistency, interface validation	Supports reliable data exchange and minimizes integration-related disruptions
Operational Continuity	Maintaining badge issuance and access functions, fallback procedures, phased transition approaches.	Reduces operational disruption and implementation risk during migration activities
Vendor Coordination	Coordination among operations, badging teams, IT personnel, vendors, and integration partners	Improves decision-making, validation efforts, and overall migration readiness

Data validation and verification were repeatedly identified as major migration considerations. Airports described conducting manual validation activities, sampling reviews, exception reporting, workflow testing, and reconciliation exercises throughout the migration process to verify accuracy and identify inconsistencies before production deployment. Some airports described performing multiple full migration cycles before acceptable data quality and reliability were achieved. Airport interviews also highlighted the operational importance of validating synchronization between systems, reviewing historical badge holder information, and identifying discrepancies prior to go-live activities.

Migration coordination also extended across multiple systems and integrations. Airports described pulling information from IDMS environments, access control systems, DAC providers, training systems, financial systems, and other platforms. Several airports noted that inconsistencies across systems significantly increased migration complexity and required additional coordination, reconciliation, and validation efforts prior to deployment.

Operational continuity requirements also influenced migration strategy decisions. Airports described balancing migration activities with the need to maintain badge issuance, credential management, access provisioning, and functional workflows. Several airports also described maintaining temporary manual procedures, fallback processes, legacy system access, or phased implementation approaches during migration and stabilization periods to reduce disruption and implementation risk.

Environment management emerged as a recurring migration consideration. Airports consistently described the use of development, testing, pre-production, and production environments. Airports reported that maintaining realistic testing environments and supporting coordination between stakeholders, IT personnel, vendors, and integration providers significantly improved migration validation and readiness efforts prior to deployment activities.

Vendor coordination is also critical throughout migration. Airports frequently referenced vendor participation in extraction activities, data mapping, transformation planning, validation support, troubleshooting, synchronization efforts, reconciliation reviews, and verification processes. Many airports noted that the implementation vendor served as the primary technical lead for migration, providing migration methodologies, templates, tools, data conversion processes, and guidance regarding data structures, field mapping, and system configuration requirements. Vendors often played a central role in identifying data quality issues, defining migration rules, supporting iterative migration testing, resolving exceptions, and coordinating cutover activities. At the same time, airports emphasized that successful migration outcomes required active airport participation because vendors typically lacked the

operational context necessary to determine which records, workflows, permissions, and historical information should be retained, modified, archived, or excluded. Vendor interviews similarly emphasized that migration complexity is frequently underestimated during early planning and that airports with a stronger understanding of legacy data conditions, business processes, and operational requirements were generally better positioned to support more stable migration outcomes and implementation coordination.

6.3 System Integration and Testing

System integration and testing significantly influence implementation stability, workflow functionality, and long-term performance. Airports consistently described IDMS environments as highly interconnected systems requiring coordination across access control platforms, DAC providers, training systems, notification platforms, financial systems, visitor management tools, and other technologies.

Several airports identified integration coordination as one of the most complex components of transition efforts. Airports described dependencies involving access provisioning, badge activation, credential synchronization, reporting functions, workflows, and automated data exchange across multiple systems. In several cases, airports noted that integration limitations within legacy environments contributed directly to fragmented workflows, manual reconciliation activities, inconsistent reporting, and broader inefficiencies supporting transition decisions.

Additional integrations frequently included training systems, financial platforms, notification systems, payment processing tools, visitor management systems, and custom interfaces. Some airports described maintaining multiple access control environments during system transition, which significantly increased coordination complexity and operational-testing requirements. Other airports described the need for custom APIs, middleware solutions, or interface management processes to support requirements not fully addressed by the core IDMS platform.

Independent SME consultants can play an important role during integration and testing activities by helping airports validate testing objectives, review test plans and scripts, coordinate user acceptance testing, and verify that operational workflows function as intended prior to deployment. Airports noted that third-party oversight can provide an additional layer of quality assurance by independently evaluating migration results, integration performance, workflow functionality, and operational readiness before production cutover occurs.

Testing Mindset: Validate testing outcomes from the perspective of all key user roles—including applicants, Trusted Agents, Authorized Signatories, administrators, and other operational users—to ensure workflows, permissions, and data function as intended after deployment.

Testing played a major role in supporting integration reliability and readiness. Airports described conducting repeated integration testing, workflow validation, migration verification, synchronization reviews, simulations, and quality-control exercises across development, testing, pre-production, and production environments. Interviewees noted that operational validation required coordination between vendors, IT personnel, functional users, access control administrators, and integration providers to ensure workflows functioned correctly under real-world conditions prior to deployment.

Airports also prioritized validating real-world workflows before deployment. Airports described validating badge issuance activities, fingerprint processing, signatory functions, reporting workflows, access provisioning, synchronization timing, and operational communication processes throughout testing. Additional airport interviews further highlighted the importance of validating API functionality,

interface reliability, data synchronization, and dependencies prior to production deployment to reduce disruption and post-implementation troubleshooting.

Environment management also influenced integration and testing coordination. Airports consistently described the use of development, testing, pre-production, and production environments to support migration, workflow testing, validation, and issue resolution throughout implementation efforts. Realistic testing environments and close coordination between operational stakeholders and technical teams significantly improved readiness and implementation stability prior to go-live.

Maintaining uninterrupted badging operations remained a constant implementation concern. Airports described balancing implementation progress with the need to maintain uninterrupted credentialing operations, access control functionality, reporting processes, and workflows. Several airports also described contingency procedures, fallback processes, phased testing approaches, and temporary manual workflows used to reduce risk during implementation and cutover activities.

Integration and testing frequently required sustained coordination between airports, vendors, IT personnel, and integration providers. Airports described ongoing collaboration involving troubleshooting, synchronization validation, workflow verification, testing support, and post-testing adjustments throughout implementation efforts. Vendors also noted that undocumented dependencies, evolving workflows, and inconsistent interface management practices often created implementation challenges that required continued coordination during deployment and stabilization efforts.

System integration and testing should be approached as major workstreams throughout IDMS transition efforts rather than isolated technical activities. Early identification of integration dependencies, realistic validation, repeated testing cycles, structured environment management, and close coordination between operational stakeholders, IT personnel, vendors, and integration providers help reduce disruption and support more stable implementation outcomes.

6.4 Operational Continuity

Operational continuity significantly influences implementation sequencing, migration planning, testing coordination, and cutover decision-making throughout IDMS transition efforts. Airports consistently emphasized that credentialing operations, badge issuance, access provisioning, reporting functions, and workflows must remain functional throughout implementation to avoid operational disruption across the airport environment.

Several airports described operational continuity planning as a major implementation consideration requiring coordination between airport security personnel, badging offices, IT organizations, operational users, vendors, access-control administrators, and executive leadership. Airports frequently balanced implementation progress with the need to maintain uninterrupted operational support for tenants, airlines, authorized signatories, airport personnel, and other operational stakeholders relying on IDMS functionality during migration and deployment efforts.

Testing coordination and phased implementation approaches also played important roles in supporting operational continuity. Airports described conducting migration validation, operational simulations, workflow testing, synchronization reviews, and integration verification across development, testing, pre-production, and production environments prior to deployment. Repeated testing helped reduce implementation risk before production cutover. Airports also identified workflow issues earlier when operational validation occurred in realistic environments.

Operational continuity considerations also influenced implementation sequencing and migration timing. Airports described coordinating migration schedules, cutover windows, integration, training timelines, operational readiness reviews, and deployment sequencing in ways that minimized disruption to daily operations. Compressed timelines or delayed implementation coordination increased risk and reduced flexibility during transition activities. Key operational continuity factors identified during IDMS transition planning are summarized in Table 4.

Table 4. Key Factors for Operational Continuity During IDMS Transitions

Vendor Communication	Vendors are involved in troubleshooting, validation, synchronization coordination, testing, and post-go-live stabilization efforts during deployment.
Stakeholder Coordination	Maintaining clear communication channels reduced confusion, improved operational readiness, and supported issue resolution.
Integration Dependencies	Testing and coordination around integrations is critical, as integration issues can affect operational workflows beyond the IDMS.
Contingency Planning	Maintaining legacy information, establishing backup procedures, and implementing phased deployment approaches reduced disruption.

Contingency planning and fallback procedures similarly emerged as recurring continuity considerations. Airports described maintaining temporary manual workflows, preserving limited access to legacy environments, establishing backup procedures, extending badging office hours, and implementing phased deployment approaches during migration and cutover periods to reduce disruption. Some airports also described maintaining access to legacy data environments after go-live to support verification and troubleshooting during stabilization efforts.

Integration dependencies also affected functional continuity planning. Airports described the need to coordinate readiness across access control systems, DAC providers, training systems, reporting platforms, and other operational technologies throughout implementation activities. Several airports emphasized that synchronization failures, interface issues, or migration inconsistencies had the potential to affect operational workflows beyond the IDMS environment itself, increasing the importance of structured testing and operational coordination.

Stakeholder communication remained central in supporting operational continuity. Airports described coordinating implementation updates, training schedules, operational notifications, signatory communication, workflow guidance, and operational support resources throughout migration and deployment activities. Several airports emphasized that maintaining clear communication channels reduced confusion, improved operational readiness, and supported more effective issue resolution during implementation efforts.

Vendor coordination similarly influenced operational continuity throughout implementation activities. Airports frequently referenced vendor participation in troubleshooting, operational validation, issue resolution, synchronization coordination, workflow testing, and post-go-live stabilization efforts during deployment. Vendor interviews also emphasized that airports with stronger operational planning processes, clearer governance structures, realistic implementation timelines, and more structured contingency planning were generally better positioned to maintain operational continuity and reduce disruption.

Taken together, the findings demonstrate that operational continuity should be treated as a central implementation objective throughout IDMS transition efforts. Structured planning, phased implementation approaches, realistic operational testing, contingency procedures, stakeholder communication, and close coordination between operational stakeholders, IT personnel, and vendors help reduce operational disruption and support more stable implementation outcomes throughout migration and deployment.

6.5 Cutover and Go-Live

Cutover and go-live activities significantly influence operational stability, implementation success, user adoption, and post-deployment system performance throughout IDMS transition efforts. Airports consistently described cutover periods as operationally sensitive phases requiring substantial coordination across operational stakeholders, IT personnel, vendors, integration providers, badging offices, and airport leadership to minimize disruption and maintain continuity throughout deployment.

Cutover and go-live planning is a phased operational process, not a single deployment event. Airports should plan on repeated migration reviews and validation, workflow testing, operational simulations, and quality control exercises—involving multiple departments and vendors—throughout the cutover and go-live process. Additional testing and stabilization activities, including operational validation, workflow adjustments, issue resolution, and training reinforcement, take place after go-live.

Testing and operational readiness played a major role in supporting successful go-live efforts. Airports described conducting repeated migration reviews, synchronization validation, operational simulations, workflow testing, access control verification, reporting validation, and quality control exercises across development, testing, pre-production, and production environments before production deployment occurred. Operational users, signatories, badging personnel, vendors, and IT teams all participated in workflow validation before final cutover. Airports consistently described this coordination as critical to deployment readiness.

Operational continuity requirements also heavily influenced cutover sequencing and deployment timing. Airports described balancing implementation schedules with the need to maintain uninterrupted badge issuance, credential-management, access provisioning, operational reporting, and tenant-support functions during go-live periods. Several airports described extending badging office hours, maintaining temporary manual workflows, implementing phased deployment strategies, or preserving limited legacy system access during deployment and stabilization to reduce operational disruption.

Post-go-live stabilization activities similarly emerged as important implementation considerations. Airports described periods of additional operational validation, troubleshooting, workflow adjustments, synchronization review, issue resolution, training reinforcement, and coordination with vendors and operational stakeholders following deployment. Some airports also described maintaining temporary access to legacy environments following deployment to support operational verification and record comparison during stabilization periods.

Stakeholder communication significantly influenced go-live readiness and deployment coordination. Airports described providing implementation updates, workflow guidance, training reminders, signatory communication, and support information during deployment to reduce confusion and improve coordination. Several airports emphasized that proactive communication improved user readiness and supported more effective issue resolution during stabilization.

Vendor coordination also played a major role throughout cutover and go-live activities. Airports frequently referenced vendor participation in deployment sequencing, troubleshooting, operational validation, migration support, issue resolution, workflow verification, and stabilization efforts during implementation. Vendor interviews similarly emphasized that airports with stronger governance structures, realistic implementation timelines, more structured operational testing, and clearer communication processes were generally better positioned to support smoother deployment and post-go-live operational stability.

During cutover and post-go-live stabilization activities, independent SME support can assist airports in monitoring implementation progress, coordinating issue resolution, validating vendor performance, facilitating stakeholder communications, and tracking corrective actions. Several airports emphasized that the period immediately following deployment often requires substantial coordination between operational users, IT personnel, vendors, and leadership teams, making dedicated project oversight particularly valuable during stabilization efforts.

Additional airport interviews highlighted the operational importance of maintaining flexibility during deployment to address unexpected workflow issues, synchronization challenges, integration discrepancies, or operational adjustments identified during production use. Several airports emphasized that implementation teams should expect continued refinement and operational coordination after initial go-live activities rather than viewing deployment as the conclusion of transition efforts.

Airports consistently emphasized that go-live periods should not be treated as isolated technical deployments. Structured testing, phased implementation approaches, stakeholder communication, contingency procedures, and close coordination between operational users, IT personnel, vendors, and integration providers were all viewed as important factors supporting smoother deployment outcomes.

To support implementation planning and coordination across the full transition life cycle, Appendix F provides an Optimized IDMS Transition Roadmap that airports may use to align planning, procurement, migration, testing, operational readiness, cutover, stabilization, and long-term support activities.

SECTION 7: CONTRACT CONSIDERATIONS AND LEGAL ISSUES

Contract structure and legal coordination played a much larger role in IDMS transitions than many airports initially expected. Airports consistently described implementation efforts as operational initiatives requiring coordination between procurement personnel, legal departments, IT organizations, airport security stakeholders, vendors, and executive leadership.

Several airports emphasized that modern IDMS contracts now extend well beyond traditional procurement language. Interviewees described growing emphasis on cybersecurity responsibilities, hosting arrangements, vendor-access controls, escalation procedures, implementation accountability, and long-term support expectations. Airports also highlighted the importance of aligning contract requirements with operational workflows, implementation sequencing, and ongoing support needs.

The findings further demonstrated that airports incorporating operational, technical, cybersecurity, and governance considerations early in contract planning were generally better positioned to reduce uncertainty and support smoother implementation efforts.

7.1 Procurement and Contracting Law

Procurement and contracting requirements significantly influence implementation sequencing, vendor selection, coordination, accountability structures, and long-term system management throughout IDMS transition efforts. Airports consistently described procurement and contracting as highly structured processes governed by airport policies, public procurement requirements, legal review procedures, organizational approval structures, and operational-risk considerations.

Several airports described procurement approaches involving formal RFP processes, cooperative purchasing agreements, phased procurement, sole-source justifications, and contract amendments associated with existing systems or airport technology environments. Airports also emphasized that procurement timelines and contracting requirements frequently influenced implementation sequencing, planning activities, vendor coordination, and overall project scheduling throughout transition efforts.

Legal review and procurement oversight also played important roles throughout contract development. Airports described coordination between procurement departments, legal stakeholders, airport security personnel, IT organizations, executive leadership, and vendor representatives throughout contract negotiations and implementation planning. Several airports emphasized that early coordination between procurement teams and legal stakeholders improved alignment between procurement documentation, requirements, implementation expectations, and long-term support obligations.

Implementation accountability and support expectations consistently emerged as major contracting considerations. Airports described the importance of clearly defining implementation responsibilities, testing obligations, migration support expectations, escalation procedures, issue resolution timelines, operational support requirements, training deliverables, and post-go-live stabilization responsibilities within contractual documentation. Several airports also emphasized that unclear accountability structures or loosely defined support expectations contributed to frustration and implementation challenges within previous environments.

Flexibility and long-term maintainability also influenced procurement and contracting discussions. Some airports described efforts to reduce excessive customization requirements, simplify implementation scope, improve maintainability, and strengthen vendor accountability language based on lessons learned from previous IDMS environments. Additional airport interviews also highlighted the

importance of clearly defining ownership responsibilities, support boundaries, implementation sequencing expectations, and escalation procedures before implementation begins.

Cybersecurity governance and operational-risk considerations increasingly influenced contract-development activities. Airports described incorporating contractual language related to hosting environments, vendor-access procedures, infrastructure responsibilities, operational security expectations, incident-response coordination, patch management responsibilities, access logging, and long-term cybersecurity support into procurement and legal review activities. Several airports emphasized the importance of aligning contractual obligations with broader airport cybersecurity governance requirements and operational risk management practices.

Continuity considerations also affected procurement and contracting activities. Airports described incorporating migration planning, implementation sequencing, testing coordination, stabilization support, contingency procedures, and operational readiness expectations into procurement documentation and implementation agreements. Several airports emphasized that continuity requirements needed to be clearly reflected within contractual language to support implementation coordination and reduce deployment risk.

Vendor interviews similarly emphasized that clearly structured procurement documentation and contractual accountability significantly improve implementation coordination and long-term alignment. Vendors noted that airports with stronger governance structures, clearer expectations, realistic implementation timelines, and more comprehensive contract language were generally better positioned to support smoother implementation and more effective issue resolution throughout the project life cycle.

A consistent theme across interviews was that procurement and contracting should align legal, technical, cybersecurity, and implementation considerations throughout the transition life cycle. Airports that established clear contractual expectations, defined implementation accountability structures, incorporated continuity considerations, and coordinated legal review activities early in the process were generally better positioned to support more stable and sustainable IDMS transition outcomes.

7.2 Regulatory and CIP Compliance

Regulatory and Critical Infrastructure Protection (CIP) compliance considerations significantly influence IDMS transition planning, implementation sequencing, operational workflows, cybersecurity governance, and long-term management throughout airport credentialing environments. Airports consistently described the need to maintain compliance alignment throughout all phases of transition while preserving continuity and supporting airport security requirements.

Several airports identified regulatory compliance limitations within legacy environments as major drivers supporting modernization and future-state requirements development. Airports described operational concerns involving audit reliability, reporting limitations, badge holder accountability, access management inconsistencies, data reconciliation challenges, signatory management issues, and difficulties maintaining accurate credentialing information within older systems. Some airports also described increased audit scrutiny or operational review activities associated with limitations in legacy operational environments.

Badge holder accountability and credential management processes also emerged as recurring compliance considerations. Airports described the importance of maintaining accurate badge holder records, validating active badge status, supporting signatory accountability, managing access privileges, coordinating CHRC activities, and maintaining reliable RapBack management processes throughout

migration and operational workflows. Additional airport interviews also highlighted the importance of identifying inactive badge holders, validating historical records, reconciling operational discrepancies, and reviewing access permissions before migration activities occur.

Audit readiness and reporting functionality were repeatedly identified as major compliance management requirements. Airports emphasized the operational importance of maintaining accurate reporting capabilities supporting badge audits, operational traceability, compliance oversight, access management accountability, and long-term record management activities. Several airports also identified the need for stronger reporting functionality, dashboard visibility, automated notifications, and operational monitoring capabilities within future-state IDMS environments.

Regulatory alignment also affected operational sequencing and implementation coordination. Airports described balancing migration schedules, cutover activities, testing coordination, badge issuance workflows, and operational continuity requirements while maintaining compliance obligations during deployment and stabilization periods. Several airports emphasized that maintaining uninterrupted credential management and access control functions during implementation activities required substantial coordination between operational stakeholders, IT personnel, vendors, and external partners.

Cybersecurity governance increasingly overlapped with compliance management activities during transition planning and implementation coordination. Airports described functional requirements involving role-based access controls, multifactor authentication, access logging, vendor-access governance, system monitoring, traceability, network segmentation, and broader alignment with airport cybersecurity governance structures. Several airports also emphasized the importance of clearly defining accountability, incident response expectations, vendor responsibilities, and hosting security controls throughout implementation and long-term operational management activities.

Operational documentation and workflow management similarly influenced compliance coordination throughout transition efforts. Airports described the need to maintain accurate procedures, reference materials, workflow documentation, signatory guidance, and training resources throughout migration and post-implementation stabilization activities to support operational consistency and regulatory alignment.

Vendor interviews similarly emphasized that regulatory and operational security expectations have become increasingly integrated into implementation planning, cybersecurity coordination, operational governance, and long-term support activities within modern IDMS environments. Vendors noted that airports are placing greater emphasis on operational traceability, audit functionality, access accountability, cybersecurity governance, and long-term compliance sustainability than in previous implementation environments.

Findings demonstrate that regulatory and CIP compliance considerations should be integrated throughout the full IDMS transition life cycle rather than addressed as isolated operational or technical tasks. Early coordination between airport security stakeholders, IT organizations, procurement personnel, legal departments, operational users, vendors, and external partners helps support stronger operational accountability, improved audit readiness, more reliable compliance management, and more effective long-term governance throughout airport IDMS environments.

7.3 Cybersecurity and Data Protection

Cybersecurity and data-protection considerations significantly influence IDMS procurement planning, implementation sequencing, operational governance, hosting decisions, vendor coordination, and long-term operational management throughout airport credentialing environments. Airports consistently

described cybersecurity governance as an increasingly important component of modern IDMS transition efforts due to the operational sensitivity of credentialing systems and the growing interconnectivity between IDMS platforms and broader airport technology environments.

Several airports described cybersecurity requirements as major factors influencing system evaluation, procurement planning, architecture decisions, and implementation coordination activities. Airports referenced operational requirements involving role-based access controls, multifactor authentication, network segmentation, access logging, system monitoring, privileged access management, vulnerability management, and broader alignment with airport cybersecurity governance structures. Several airports also emphasized the importance of coordination between airport security departments and IT organizations to ensure cybersecurity expectations were incorporated into procurement documentation, implementation planning, and operational workflows early in the transition life cycle. Common cybersecurity and data protection considerations identified during IDMS transition planning are summarized in Table 5.

Table 5. Cybersecurity and Data Protection Considerations for IDMS Transitions

Authentication	MFA requirements for airport users, administrators, signatories, and vendor access.
Role-based access	Least-privilege/zero trust permissions for Trusted Agents, admins, IT, vendors, and external users
Vendor access	Remote-access method, approval process, logging, monitoring, and emergency access
Hosting model	Cloud, on-premises, hybrid, SaaS, data location, backup, and responsibility boundaries
Logging and Monitoring	User activity logs, administrative actions, failed logins, access changes, audit trails
Patch Management	Responsibility for OS, application, database, and integration updates
Data Protection	Encryption, PII handling, retention, backups, export rights, and destruction at contract end
Incident Response	Notification timelines, roles, escalation paths, vendor responsibilities, evidence preservation

Integration security and system interoperability also emerged as important cybersecurity considerations during IDMS transitions. Airports noted that modern IDMS platforms frequently exchange information with access control systems, CBT systems, DACs, identity providers, and other operational platforms through APIs and automated interfaces. As new integrations are implemented and legacy interfaces are retired, airports should evaluate API security controls, authentication mechanisms, authorization processes, API key management, token handling, and encryption requirements. Several stakeholders noted that legacy APIs, unused interfaces, or obsolete integrations left active after implementation can create unnecessary attack surfaces and increase cybersecurity risk.

Certificate management and encryption compatibility similarly require careful evaluation throughout implementation and migration activities. Airports described the importance of validating TLS/SSL

certificates, secure communication protocols, and encryption methods used between integrated systems. Particular attention should be given to ensuring that credential and badge media encryption requirements remain compatible with existing access control systems and downstream operational platforms. Failure to validate encryption and certificate requirements during testing can result in both operational disruptions and security vulnerabilities following deployment.

Network-security reviews also play an important role during transition activities. New software, hardware, cloud services, and integrations may require additional network communications, firewall rules, ports, and services. Airports should verify that only required ports and services are enabled and that legacy communications associated with retired systems are removed following cutover activities. Several stakeholders noted that administrative access ports, remote support connections, web services, and integration pathways should be reviewed during implementation to minimize unnecessary exposure and support broader airport cybersecurity governance objectives.

Logging, monitoring, and audit trail continuity were also identified as critical implementation considerations. System migrations can inadvertently disrupt security monitoring, dashboard reporting, audit logging, or event management integrations if dependencies are not fully documented and tested. Airports emphasized the importance of validating that user activity, administrative actions, access changes, synchronization events, and other operational transactions continue to be captured and retained throughout migration, testing, deployment, and post-implementation stabilization activities. Maintaining accurate logging and audit capabilities supports operational accountability, incident response activities, regulatory compliance, and long-term cybersecurity monitoring.

Hosting environments and infrastructure management responsibilities also emerged as recurring cybersecurity considerations. Airports described evaluating cloud hosted systems, on-premises environments, hybrid architectures, remote access capabilities, infrastructure ownership responsibilities, and vendor support models throughout planning and procurement activities. Several airports emphasized the importance of clearly defining operational responsibilities associated with hosted environments, vendor-access procedures, patch management expectations, incident response coordination, and long-term operational security obligations before implementation activities begin. Additional airport interviews also highlighted the operational importance of understanding third-party dependencies and external hosting considerations throughout implementation planning activities.

Vendor-access governance similarly played a significant role throughout cybersecurity planning and operational coordination activities. Airports described operational concerns related to privileged access management, remote support procedures, production environment access, access logging, monitoring expectations, escalation procedures, and operational accountability associated with vendor supported environments. Several airports emphasized that clearly defined vendor-access controls and operational security responsibilities became increasingly important within modern cloud-hosted and remotely supported operational environments.

Data protection and operational accountability also influenced cybersecurity management discussions throughout implementation. Airports described the need to maintain accurate operational records, preserve access management traceability, support operational monitoring, and protect sensitive credential management information throughout migration, integration, testing, and post-implementation operations. Several airports also emphasized the importance of aligning operational security practices with broader airport governance structures and long-term operational risk management activities.

Cybersecurity coordination additionally affected implementation sequencing, migration planning, testing, and operational continuity efforts. Airports described balancing operational security requirements with migration schedules, integration coordination, remote access needs, operational

testing, and deployment timelines throughout implementation efforts. Several airports emphasized that cybersecurity review frequently influenced procurement schedules, implementation sequencing, and infrastructure decisions during transition projects.

Operational documentation and governance processes also emerged as important cybersecurity considerations. Airports described maintaining operational procedures, incident response guidance, vendor-access documentation, access management workflows, escalation procedures, and operational reference materials supporting long-term operational security coordination following implementation activities.

Vendor interviews similarly emphasized that cybersecurity expectations have become increasingly integrated into all phases of IDMS implementation and long-term operational support. Vendors noted that airports are placing substantially greater emphasis on operational security governance, vendor accountability, hosting controls, privileged-access management, monitoring capabilities, and operational traceability than in previous implementation environments. Vendors also stated that airports with stronger governance structures, clearer operational accountability models, and more mature cybersecurity coordination processes were generally better positioned to support more stable and sustainable long-term operational environments.

Cybersecurity and data protection considerations should be integrated throughout the full IDMS transition life cycle rather than addressed as isolated technical requirements. Early coordination between airport security stakeholders, IT organizations, procurement personnel, legal departments, operational users, vendors, and external service providers helps support stronger operational security governance, improved accountability, more reliable operational coordination, and more sustainable long-term management of airport IDMS environments.

7.4 Vendor Access and Control Rights

Vendor access and control rights significantly influence cybersecurity governance, operational accountability, implementation coordination, continuity, and long-term system management throughout IDMS environments. Airports consistently described the need to carefully manage vendor access to systems, credential management environments, infrastructure resources, and sensitive data throughout implementation and post-deployment.

Several airports described vendor-access management as an increasingly important consideration due to the growing use of cloud-hosted systems, remote support models, integrated environments, and externally managed infrastructure components within modern IDMS deployments. Airports frequently referenced requirements involving privileged-access management, role-based permissions, remote access procedures, monitoring expectations, access logging, and operational accountability controls throughout implementation and long-term activities.

Operational governance and cybersecurity coordination also played major roles in vendor-access management activities. Airports described coordination between airport security personnel, IT organizations, cybersecurity stakeholders, procurement departments, legal teams, and vendor representatives to establish operational access procedures, define escalation protocols, clarify support boundaries, and align vendor responsibilities with broader airport cybersecurity governance structures. Clearly defined vendor-access procedures became increasingly important as airports expanded into cloud-hosted and remotely managed environments. Several airports also identified growing concern regarding third-party integration dependencies.

Contractual language and procurement documentation also influenced vendor-access governance activities. Airports described incorporating operational security expectations, infrastructure responsibilities, monitoring requirements, access limitations, support procedures, incident response coordination, and operational accountability provisions into procurement and contract development. Several airports emphasized the importance of clearly defining vendor responsibilities related to production environment access, troubleshooting, infrastructure management, and long-term support coordination before implementation begins.

Implementation sequencing and continuity considerations similarly affected vendor-access management. Airports described balancing the need for vendor support during migration, testing, integration, troubleshooting, and deployment activities with broader operational security and operational accountability requirements throughout transition efforts. Several airports also emphasized the importance of maintaining visibility into vendor activities, monitoring functional access, and coordinating support activities throughout implementation and stabilization periods.

Additional airport interviews highlighted the importance of maintaining clearly identified vendor points of contact, escalation procedures, and operational support structures throughout implementation and post-deployment activities. Some airports described situations where unclear support boundaries or inconsistent coordination created delays or increased troubleshooting complexity during implementation efforts.

Cybersecurity governance further influenced vendor-access controls and operational accountability expectations. Airports described requirements involving multifactor authentication, access logging, privileged-access restrictions, network segmentation, remote access monitoring, incident response coordination, and alignment with airport cybersecurity governance structures throughout implementation and operational activities. Several airports also emphasized the importance of maintaining traceability and preserving accountability for changes affecting production environments throughout the life cycle of the system.

Vendor interviews similarly emphasized that coordination and clearly defined governance structures significantly improve implementation support and long-term management. Vendors noted that airports with stronger governance processes, more clearly defined operational responsibilities, structured access-management procedures, and realistic support expectations were generally better positioned to support smoother implementation coordination and long-term operational stability.

Collectively, the findings demonstrate that vendor-access and control-rights considerations should be integrated into procurement planning, cybersecurity governance, implementation coordination, and long-term operational-management throughout IDMS transition efforts. Clearly defined responsibilities, structured access-management procedures, monitoring capabilities, escalation protocols, and coordinated governance help support stronger accountability, improved cybersecurity coordination, and more sustainable long-term environments.

7.5 Operational Risk and Liability During Transition

Operational risk and liability considerations significantly influence implementation planning, continuity coordination, governance activities, vendor accountability, and long-term system management throughout IDMS transition efforts. Airports described transition as operationally sensitive initiatives requiring coordination across airport security personnel, IT organizations, procurement departments, legal stakeholders, users, vendors, and executive leadership to reduce implementation risk and maintain continuity throughout deployment.

Several airports described operational risk as extending beyond technical implementation concerns and affecting credential management functions, access provisioning, badge issuance activities, reporting capabilities, audit readiness, workflows, and broader airport security operations. Airports frequently emphasized the importance of maintaining uninterrupted functionality while balancing migration activities, testing coordination, integration sequencing, cybersecurity governance, and implementation timelines throughout deployment efforts.

Implementation sequencing and continuity planning also played major roles in reducing operational risk. Airports described balancing deployment schedules with the need to maintain badge holder processing, access control functionality, reporting, tenant coordination, and credential management activities throughout migration and cutover periods. Several airports emphasized that compressed timelines, delayed coordination activities, unresolved integration issues, or inadequate testing significantly increased risk during implementation efforts.

Contingency planning and fallback operational procedures similarly emerged as recurring operational risk considerations. Airports described maintaining temporary manual workflows, preserving access to legacy systems, implementing phased deployment approaches, extending support coverage, and establishing backup procedures during migration and cutover activities to reduce disruption and implementation risk. Some airports also described maintaining temporary redundancies and post-deployment verification activities during stabilization periods to support continuity and issue resolution.

Contractual accountability and vendor coordination also significantly influenced operational risk management discussions. Airports described the importance of clearly defining implementation responsibilities, escalation procedures, operational support expectations, migration accountability requirements, testing obligations, and stabilization support responsibilities throughout procurement and contract development activities. Several airports emphasized that unclear responsibilities or inconsistent vendor coordination contributed to implementation delays, troubleshooting challenges, and uncertainty within previous implementation environments.

Cybersecurity governance further influenced operational liability considerations throughout transition activities. Airports described concerns involving privileged-access management, vendor-access controls, traceability, incident response coordination, monitoring expectations, hosting responsibilities, and broader alignment with airport cybersecurity governance structures throughout implementation and long-term activities. Several airports emphasized the importance of clearly defining accountability structures and escalation procedures before deployment.

Stakeholder communication and governance coordination also affected operational risk management. Airports described maintaining coordination between airport security personnel, IT organizations, vendors, procurement stakeholders, legal departments, and executive leadership to improve issue resolution, reduce uncertainty, and support more effective decision-making during implementation. Additional interviews highlighted the importance of clear communication channels and governance structures during migration and stabilization.

Vendor interviews similarly emphasized that risk is frequently increased when implementation expectations, governance structures, responsibilities, or escalation procedures are not clearly defined early in the transition life cycle. Vendors noted that airports with stronger governance processes, more realistic implementation timelines, structured testing activities, and clearly defined operational-accountability models were generally better positioned to support smoother implementation coordination and reduce disruption throughout deployment efforts.

Risk and liability considerations should be integrated throughout procurement planning, implementation sequencing, cybersecurity coordination, operational governance activities, and long-term support planning throughout IDMS transition efforts. Structured governance processes, realistic implementation planning, contingency procedures, operational accountability frameworks, and close coordination between stakeholders, IT personnel, vendors, procurement teams, and legal stakeholders help reduce disruption and support more stable implementation outcomes.

SECTION 8: TRAINING AND DOCUMENTATION

Training and documentation consistently emerged as major implementation factors throughout airport interviews. Airports described IDMS transitions as operational changes that affected daily workflows, reporting responsibilities, signatory coordination, access management procedures, and credentialing activities across multiple stakeholder groups.

Several airports emphasized that successful implementation required coordination between badging offices, airport security personnel, operational users, IT organizations, vendors, signatories, and executive leadership. Airports also described the importance of aligning training with real-world workflows, implementation timing, and day-to-day credential-management responsibilities.

Airports consistently emphasized that long-term system effectiveness depended on continued training, documentation updates, workflow refinement, and knowledge retention after deployment occurred.

8.1 Training Program Development

Training program development significantly influences operational readiness, user adoption, workflow consistency, compliance coordination, and long-term effectiveness throughout IDMS transition efforts. Airports consistently described training activities as operationally critical components of implementation efforts due to the broad range of stakeholders interacting with credential management systems throughout airport environments.

Several airports described training activities involving airport security personnel, badging-office staff, operational users, IT organizations, authorized signatories, tenant representatives, access control administrators, and executive stakeholders throughout implementation and post-deployment activities. Airports frequently utilized combinations of vendor-led instruction, internal training, train-the-trainer approaches, workflow demonstrations, operational-reference materials, and hands-on exercises throughout transition efforts.

Key Considerations for Developing Your Training Program

- Involve all end users in training, including airport security personnel, badging office staff, operational users, IT organizations, authorized signatories, tenant representatives, access control administrators, and executive stakeholders
- Use a range of trianing methods, including vendor-led instruction, internal training, train-the-trainer sessions, workflow demonstrations, operational reference materials, and hands-on exercises
- Structure training around real-world credential management processes and each user group's day-to-day responsibilities rather than focusing only on system functionality
- Align training timing with implementation sequencing and go-live
- Use phased training and provide reinforcement when training occurs early
- Continue training after deployment through refresher secctions, updated guidance, workflow demonstrations, and ongoing user support

Operational workflow alignment consistently emerged as a major training consideration. Airports described the importance of structuring training activities around real-world credential management processes, badge issuance workflows, signatory functions, reporting activities, access provisioning, fingerprint processing, and coordination responsibilities rather than focusing solely on system functionality. Users responded best to hands-on workflow training aligned with daily responsibilities. Timing also contributed to success.

Implementation timing influenced training effectiveness. Some airports described situations where training conducted too early in the implementation process reduced user retention and required

additional reinforcement closer to go-live activities. Other airports emphasized the value of phased training approaches aligned with implementation sequencing, migration activities, workflow readiness, and deployment schedules throughout transition efforts.

Operational complexity and workflow changes similarly affected training requirements. Airports described transitions involving new approval processes, updated workflows, enhanced reporting functionality, dashboard-management tools, automated processes, revised signatory coordination procedures, and broader workflow changes compared to legacy environments. Several airports emphasized that users frequently required additional support and reinforcement while adapting to updated workflows and expectations during implementation and stabilization.

Additional airport interviews highlighted the operational importance of supporting training continuity following implementation activities. Some airports described maintaining refresher training, updated guidance, workflow demonstrations, and ongoing user support resources following deployment to support long-term consistency and compliance management.

Vendor coordination also played a major role throughout training. Airports frequently referenced vendor participation in workflow demonstrations, guidance, troubleshooting support, implementation coordination, and post-go-live assistance throughout transition efforts. Vendor interviews similarly emphasized that user adoption and readiness depend heavily on realistic workflow training, structured implementation coordination, and continued support throughout stabilization periods following deployment.

Training program development should be approached as an operational-readiness process rather than a standalone implementation task. Airports that aligned training with workflows, implementation timing, stakeholder responsibilities, and long-term operational support objectives were generally better positioned to support smoother user adoption, reduce disruption, and improve long-term system effectiveness throughout IDMS transition efforts.

8.2 Documentation Requirements

Documentation requirements significantly influence consistency, compliance coordination, workflow management, training continuity, and long-term sustainability throughout IDMS transition efforts. Airports consistently described the need to maintain accurate documentation throughout planning, implementation, migration, testing, deployment, and post-implementation stabilization to support continuity and preserve institutional knowledge.

Several airports described maintaining documentation related to badge issuance workflows, signatory procedures, access management processes, migration, operational security procedures, escalation protocols, integration coordination, reporting responsibilities, and implementation governance activities throughout transition efforts. Airports also emphasized the importance of maintaining updated operational reference materials supporting both implementation and long-term operational management following deployment.

Operational workflow documentation also emerged as a recurring requirement. Airports described documenting revised workflows, updated approval structures, automation procedures, operational dependencies, reporting activities, and credential management responsibilities associated with newer IDMS environments. Several airports emphasized that documentation updates became particularly important when processes changed significantly during implementation or when automation replaced previously manual activities.

Compliance management activities similarly influenced documentation requirements. Airports described maintaining records, workflow guidance, audit support materials, signatory references, operational procedures, and credential management documentation supporting TSA requirements, badge holder accountability activities, access management coordination, and long-term compliance management responsibilities throughout transition and operational activities.

Building Your Document Library

Maintaining accurate documentation supports continuity and preserves institutional knowledge. Airports should consider documenting the following items during implementation:

- Operational workflows, approval structures, automation procedures, reporting activities, credentialing responsibilities
- Compliance management, audit support materials, TSA requirements, operational procedures, access management guidance, badgeholder activities
- Implementation activities, migration procedures, testing plans, cutover and fall-back documentation, operational readiness checklists, stabilization support materials
- Vendor user guidance, escalation procedures, and training and troubleshooting resources

Implementation coordination and continuity planning also required substantial documentation activities. Airports described maintaining migration procedures, testing plans, environment management guidance, cutover sequencing documentation, fallback operational procedures, operational readiness checklists, and stabilization support materials throughout implementation efforts. Several airports emphasized that maintaining clearly documented operational procedures improved implementation coordination and reduced operational confusion during deployment.

Additional airport interviews also highlighted the importance of maintaining updated documentation following implementation tasks. Some airports described ongoing updates to operational reference materials, workflow documentation, user guidance, escalation procedures, training resources, and governance documentation following deployment activities to support long-term consistency and future operational adjustments.

Vendor coordination similarly influenced documentation management activities. Airports frequently referenced vendor-provided implementation documentation, workflow guidance, system reference materials, troubleshooting resources, escalation documentation, and operational support procedures throughout implementation and post-go-live activities. Vendor interviews also emphasized that airports maintaining stronger documentation management practices were generally better positioned to support long-term continuity and reduce dependency on informal institutional knowledge.

Overall, the findings demonstrate that documentation requirements should support operational continuity, compliance coordination, workflow management, implementation governance, training continuity, and long-term sustainability throughout IDMS transition efforts. Airports that maintained structured documentation management practices throughout implementation and operational activities were generally better positioned to support more consistent performance and long-term system management.

8.2 Change Management

The Importance of Change Management for Effective Implementation: IDMS transitions affect existing workflows, reporting activities, access procedures, and day-to-day responsibilities across multiple stakeholder groups. These transitions often require users to adapt not only to new technology but also to revised processes and workflow expectations. Airports that take a proactive approach to change management through strong communication, workflow alignment, implementation timelines, and vendor coordination report having a strong transition and adoption.

Change-management significantly influences user adoption, coordination, workflow consistency, stakeholder engagement, and long-term implementation success throughout IDMS transition efforts. Airports consistently described IDMS transitions as changes affecting credential management workflows, reporting activities, signatory coordination, access management procedures, communication, and day-to-day responsibilities across multiple stakeholder groups throughout airport environments.

Several airports described adjustments involving updated workflows, revised approval processes, automation changes, reporting modifications, dashboard management tools, signatory coordination procedures, and new responsibilities associated with implementation of newer IDMS environments. Airports frequently emphasized that transitions required users to adapt to both new technology platforms and revised processes and workflow expectations throughout implementation and stabilization activities.

Stakeholder engagement also played a major role throughout change management activities. Airports described coordination involving airport security personnel, badging offices, IT organizations, users, signatories, tenant representatives, executive leadership, vendors, and access control administrators throughout planning and implementation activities. Several airports emphasized that early stakeholder involvement improved alignment, reduced implementation resistance, and supported more effective workflow adoption during transition efforts.

Communication activities similarly influenced change management effectiveness. Airports described providing implementation updates, workflow guidance, notifications, training reminders, signatory communication, operational-support information, and deployment-status coordination throughout migration and implementation activities. Several airports emphasized that maintaining clear communication channels helped reduce confusion and improve user readiness throughout deployment and stabilization periods.

Workflow alignment also affected user adoption throughout transition efforts. Airports described the value of systems supporting more intuitive interfaces, step-by-step workflows, integrated dashboard functionality, improved reporting visibility, and stronger automation capabilities compared to legacy environments. Several airports also noted that users adapted more effectively when implementation activities were aligned with realistic workflow requirements and responsibilities.

Implementation timing and sequencing further influenced change-management coordination. Some airports described phased implementation approaches, staged workflow transitions, operational-readiness activities, and progressive deployment coordination designed to reduce disruption and improve stakeholder adaptation throughout implementation efforts. Additional airport interviews also highlighted the importance of maintaining flexibility to address workflow adjustments and concerns identified during deployment activities.

Vendor coordination also played a major role throughout change management activities. Airports frequently referenced vendor participation in workflow demonstrations, guidance, user support, troubleshooting coordination, and post-go-live stabilization efforts during implementation. Vendor interviews similarly emphasized that user adoption and adjustment frequently continue beyond initial deployment and require ongoing coordination between airports and vendors following go-live.

Change management should be approached as a long-term operational coordination process rather than a short-term implementation activity. Airports that maintained strong stakeholder engagement, realistic workflow alignment, structured communication practices, phased operational coordination, and ongoing operational support activities were generally better positioned to support smoother user adoption and long-term stability throughout IDMS transition efforts.

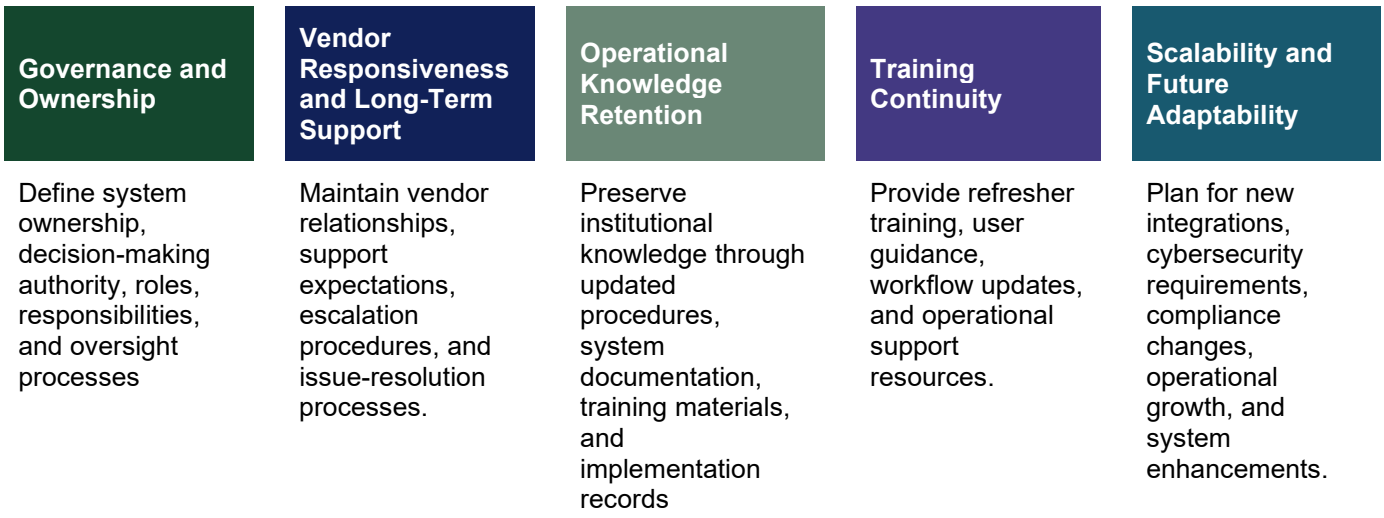
8.4 Ongoing Support and Knowledge Retention

Go-live is not the finish line. Airports and vendors consistently emphasized that long-term IDMS success depends on sustained governance, vendor coordination, knowledge retention, and user support after implementation is complete. Maintaining clear ownership, current documentation, ongoing training, and structured support processes helps airports preserve operational continuity, support compliance requirements, and adapt to evolving operational and technology needs over time.

Ongoing support and knowledge retention activities significantly influence long-term functional stability, compliance management, workflow continuity, vendor coordination, and overall system sustainability following IDMS implementation activities. Airports consistently emphasized that management responsibilities continue well beyond go-live and require structured coordination across operational stakeholders, IT organizations, vendors, airport leadership, and compliance management personnel throughout the life cycle of the system.

Several airports described ongoing operational support involving workflow refinement, troubleshooting coordination, reporting management, operational security oversight, user support activities, vendor coordination, escalation management, compliance monitoring efforts, and operational documentation updates following deployment. Airports also emphasized the importance of maintaining clearly identified ownership structures and governance processes supporting long-term management after implementation concluded. The major elements supporting long-term IDMS sustainability are summarized in Figure 7.

Figure 7. Five Pillars of Long-Term IDMS Sustainability



Vendor responsiveness and long-term support coordination also emerged as major operational considerations. Several airports contrasted legacy environments involving delayed issue resolution, inconsistent communication, unresolved concerns, and reactive support approaches with newer support environments emphasizing proactive coordination, stronger engagement, and more structured escalation management processes. Additional airport interviews also highlighted the importance of maintaining clearly identified vendor points of contact and escalation procedures throughout long-term activities.

Operational knowledge retention similarly influenced long-term system management discussions. Airports described the need to preserve institutional knowledge related to workflows, reporting procedures, signatory coordination, migration history, integration dependencies, operational security

procedures, and implementation decisions throughout staffing changes and evolving environments. Several airports emphasized that maintaining updated documentation, structured training, operational-reference materials, and governance procedures significantly improved long-term continuity and reduced dependency on informal knowledge transfer.

Training continuity and reinforcement also remained important after implementation activities concluded. Airports described maintaining refresher training, workflow demonstrations, updated user guidance, operational support resources, and compliance-related instruction throughout ongoing activities to support workflow consistency and operational accountability. Some airports also identified dedicated operational support roles or governance structures established following implementation to coordinate long-term management activities.

Scalability and future adaptability also influenced long-term support planning. Airports described ongoing coordination related to future integrations, modernization initiatives, expansion, cybersecurity requirements, evolving compliance expectations, and future workflow adjustments throughout long-term operational planning activities. Several airports emphasized that implementation decisions made during transition activities directly affected long-term flexibility and future supportability within airport environments.

Vendor interviews similarly emphasized that long-term success depends heavily on ongoing coordination between airports and vendors following implementation activities. Vendors noted that airports with stronger governance structures, clearer ownership, structured documentation practices, realistic support expectations, and continued training coordination were generally better positioned to maintain stability and adapt to evolving requirements over time.

Ongoing support and knowledge retention should be treated as core management responsibilities throughout the life cycle of airport IDMS environments. Structured governance processes, continued training activities, operational documentation management, vendor coordination, and preservation of institutional knowledge help support long-term continuity, stronger compliance management, and more sustainable environments following IDMS transition efforts.

SECTION 9: UPDATES TO PARAS 0038 – AIRPORT GUIDANCE FOR IDMS

PARAS 0067 is intended to supplement, not replace, PARAS 0038 – Airport Guidance for Identity Management Systems. The research identified specific opportunities to update PARAS 0038 to reflect current transition practices, cybersecurity expectations, implementation complexity, and long-term IDMS management considerations.

The recommendations below are mapped to the structure of PARAS 0038. Where PARAS 0038 addresses a topic, the recommendation is to revise or expand the existing guidance. New subsections are proposed only where the current guidebook does not provide a clear location for transition-specific findings.

9.1 Addition of New Subsections

PARAS 0038 provides a strong foundation for planning, procuring, and implementing an IDMS. However, several transition-specific topics identified through PARAS 0067 do not have a clear home within the existing structure. These topics include assessing when an existing IDMS should be replaced, establishing transition governance, developing a formal business case, planning for operational continuity, and managing post-go-live stabilization. The proposed subsections outlined in Table 6 would allow these findings to be incorporated without substantially reorganizing the guidebook.

Table 6. Proposed Additions to PARAS 0038

Proposed Subsection	Proposed Location in PARAS 0038	Recommended Content
Assessing the Need to Transition an Existing IDMS	After Section 3.1, Assessing the Need for an IDMS	Address the cumulative conditions that may justify replacement or transition of an existing IDMS, including declining vendor support, operational performance deficiencies, integration limitations, cybersecurity and compliance gaps, aging infrastructure, and the risks associated with maintaining the status quo. The assessment should translate these conditions into site-specific evidence, operational impacts, risks, and future-state requirements.
Governance, Decision Authority, and Change Management	After Section 3.7.2, Stakeholders	Define executive sponsorship, project leadership, decision-making authority, cross-functional governance, stakeholder responsibilities, escalation procedures, communication practices, and change-management activities. Emphasize that an IDMS transition is an organization-wide operational initiative rather than an isolated technology project.
Business Case Development	After Section 3.8, Cost Considerations	Provide guidance for comparing transition costs with the operational, financial, cybersecurity, compliance, and supportability risks of maintaining the existing environment. Include staff resource impacts, life cycle costs, operational inefficiencies, risk-reduction benefits, and long-term return on investment.
Contract-Specific Subsections	Within Section 4.5, Contract Considerations	Organize the section into focused subsections addressing service levels and support, cybersecurity and data protection, vendor access and control rights, data ownership, termination and transition assistance, operational risk and liability, warranty requirements, and long-term life cycle commitments.

Proposed Subsection	Proposed Location in PARAS 0038	Recommended Content
Operational Continuity and Go/No-Go Readiness	Within Section 5.4, Testing and Cutover, before the cutover discussion	Address continuity planning, temporary and manual fallback processes, parallel operations where appropriate, operational-readiness criteria, decision authority, rollback thresholds, stakeholder communications, and minimum conditions that should be satisfied before production cutover.
Post-Go-Live Stabilization and Knowledge Retention	Within Section 5.6, Project Closeout, before the existing maintenance subsection	Address stabilization periods, issue tracking, vendor support following deployment, operational acceptance, documentation handoff, knowledge transfer, refresher training, support escalation, and preservation of institutional knowledge. Existing maintenance and end-of-life subsections may be renumbered as needed.

These proposed additions address areas that have become more important as IDMS platforms have evolved into highly integrated enterprise systems. They are intended to complement the existing planning and implementation guidance rather than duplicate topics already addressed in PARAS 0038.

9.2 Revise Existing Sections

Several PARAS 0038 sections already address topics that were also examined under PARAS 0067, including data migration, testing, cutover, contract considerations, and long-term system management. In these cases, the existing sections should be revised rather than supplemented with entirely new material. The recommended revisions outlined in Table 7 focus on incorporating current transition practices, clarifying responsibilities, and strengthening guidance related to operational readiness, cybersecurity, validation, and vendor accountability.

Table 7. Proposed Revisions to PARAS 0038

PARAS 0038 Section	Recommended Revision
Sections 3.6 and 5.3, Data Reconciliation, Cleanup, Staging and Migration/Data Migration	Clearly distinguish planning-stage data readiness from implementation-stage migration execution. Expand the guidance to address source system identification, data ownership, duplicate and inactive records, access privilege validation, signatory and RapBack information, repeated migration test cycles, reconciliation, exception handling, quality control, legacy data retention, and fallback requirements.
Section 4.5, Contract Considerations	Broaden the section beyond contract type and payment schedules. Clearly define airport, vendor, integrator, and third-party responsibilities for implementation, migration, cybersecurity, system access, data protection, support, issue resolution, termination assistance, and long-term lifecycle management.
Section 5.4, Testing and Cutover	Reorganize the section around end-to-end operational testing, integration validation, realistic user workflows, migration validation, operational continuity, go/no-go decision-making, cutover coordination, rollback triggers, issue management, and post-go-live stabilization.
Section 6, Summary of Best Practices	Update the summary to include transition-specific practices involving governance, current-state assessment, repeated migration validation, operational continuity, vendor accountability, cybersecurity coordination, realistic workflow testing, documentation, and post-go-live support.

PARAS 0038 Section	Recommended Revision
Section 7, Emerging Trends and Innovation	Update the section to reflect current developments involving cloud-hosted and web-based IDMS platforms, configurable system environments, workflow automation, increased interoperability, cybersecurity governance, evolving vendor-service models, and long-term system adaptability. Retain speculative technologies only where they remain relevant and supported by current industry conditions.

These revisions would preserve the original subject matter and organization of PARAS 0038 while updating the guidance to reflect the implementation challenges and practices reported by airports during the PARAS 0067 research.

9.1 Expand Existing Guidance

Other findings from PARAS 0067 are best incorporated by expanding existing guidance rather than creating new subsections or substantially rewriting current sections. The recommendations outlined in Table 8 provide additional depth in areas already addressed by PARAS 0038, including current-state evaluation, stakeholder participation, system integrations, technical requirements, procurement, training, and life cycle management.

Table 8. Proposed Expansions to PARAS 0038

PARAS 0038 Section	Recommended Expansion
Section 3.3, Identification of Existing Processes and Systems	Expand the current-state evaluation to include system reliability, vendor-support status, browser and equipment dependencies, data quality, reporting and audit capabilities, operational workflows, stakeholder experience, cybersecurity conditions, integration dependencies, and desired future-state capabilities.
Section 3.4, Integration Considerations	Add guidance related to integration ownership, synchronization timing, interface reliability, data exchange, third-party dependencies, middleware and APIs, testing responsibilities, maintenance impacts, and coordination among vendors and integration providers.
Section 3.5, IT Systems and Requirements	Expand cybersecurity and hosting guidance to address cloud, on-premises, and hybrid environments; role-based access controls; multi-factor authentication; privileged and vendor access; logging and monitoring; network segmentation; patch management; incident-response coordination; and infrastructure and hosting responsibilities.
Section 3.7, Staff and Stakeholders	Broaden the stakeholder discussion to include executive leadership, airport security, badging personnel, IT and cybersecurity organizations, operations, procurement, legal, finance, access-control administrators, authorized signatories, tenants, airlines, vendors, integration providers, and federal, state, and local partners.
Section 3.8, Cost Considerations	Add potential transition costs involving staff time, data cleanup and validation, accelerated schedules, licensing, multi-factor authentication, hardware and peripheral replacement, workspace modifications, badge encoding, storage, third-party integrations, parallel operations, training, stabilization, and long-term support.
Sections 3.9 and 3.10, Technical Requirements and Operational and Process Requirements	Organize requirements into functional, technical, compliance, and performance categories. Emphasize measurable requirements, workflow alignment, operational-user participation, scalability, supportability, reporting, reliability, and the use of vendor-supported configuration before custom software development.

PARAS 0038 Section	Recommended Expansion
Sections 4.1 through 4.3, Procurement Documents, Vendor Evaluation and Selection, and Scope of Work Development	Expand procurement guidance to address migration, testing, operational continuity, cybersecurity, data ownership, vendor access, training, documentation, stabilization, and post-implementation support. Vendor evaluation should consider airport-specific experience, proposed personnel, implementation history, cybersecurity posture, migration and integration capability, support responsiveness, workflow-based demonstrations, and peer-airport references.
Sections 5.1 and 5.2, Schedule and Key Milestones and Environments	Expand schedule guidance to address dependencies, airport staffing constraints, phased implementation, governance reviews, readiness milestones, cutover preparation, and stabilization. Clarify the purpose and expected fidelity of development, testing, pre-production or staging, and production environments.
Section 5.5, Training	Expand training guidance by user group and operational responsibility. Address hands-on and workflow-based instruction, timing near go-live, train-the-trainer approaches, site-specific materials, refresher training, post-deployment reinforcement, and continued user support.
Sections 5.6.1 and 5.6.2, Maintenance and End-of-Life Considerations	Expand long-term guidance to address governance following implementation, vendor-support coordination, documentation updates, performance monitoring, change control, patch and upgrade testing, knowledge retention, vendor-roadmap monitoring, and planned transition before end-of-life conditions create operational urgency.

The recommended expansions are intended to add transition-specific detail and current operational context to the existing guidance. They would help airports apply PARAS 0038 not only when implementing an IDMS for the first time, but also when replacing or modernizing an established IDMS environment.

9.4 Final Observations

The proposed revisions preserve the original organization and purpose of PARAS 0038 while incorporating transition-focused findings from PARAS 0067. Most recommendations can be implemented through targeted revisions or expansions to existing planning, procurement, implementation, and life cycle management sections. New subsections are recommended only where PARAS 0038 does not currently provide a clear home for transition assessment, governance, business case development, contract risk allocation, operational-continuity readiness, or post-go-live stabilization.

APPENDIX A: QUESTIONS FOR VENDOR INTERVIEWS

Category	Key Questions
1. Airports list	List of airports where the vendor has displaced legacy IDMS. • Did the airport make the reason clear for the replacement? • Were there any specific timelines or external factors that were driving the timeline for replacement?
2. Project & Transition Planning	• What implementation methodology do you follow (e.g., Agile, Waterfall, hybrid)? • How do you manage project risks, scope changes, and unexpected delays? • What is the high-level project timeline and key milestones for the transition? • How do you coordinate with multiple airport stakeholders (security, IT, HR, tenants)? • Will you provide a dedicated project manager and technical lead? • What is your change management process during the migration?
3. Procurement	• How will you ensure the new IDMS architecture meets current and future airport needs? • What is your approach for high availability and disaster recovery design? • How will you handle multi-tenant requirements (airlines, vendors, contractors)? • How will the system integrate with existing airport systems such as access control, HR/payroll, badge printing, visitor management? • Will custom APIs or middleware be required, and who maintains them?
4. Environments, Data Migration & Integration	• What is your strategy for migrating user records, access permissions, and historical data? • How will you clean and transform legacy data for compatibility with the new IDMS? • What processes will you use to validate data accuracy and completeness? • How do you ensure minimal downtime or data loss during the cutover?
5. Access Control & Security	• How will you ensure the new system meets TSA, FAA, and local regulatory requirements? • What is your approach to protecting Personally Identifiable Information (PII) during migration? • How will encryption and key management be implemented? • How will you handle secure authentication (MFA, biometrics, smart cards)? • What is your process for regular security testing and penetration testing?
6. Compliance & Regulatory Considerations	• What types of testing will you perform (unit, system, integration, user acceptance)? • How will you ensure access control rules and role-based permissions migrate correctly? • What performance and load testing will be performed to simulate peak airport operations? • How will you track and resolve defects discovered during testing?
7. Operational Impact & Training	• Will you provide technical documentation and system architecture diagrams? • What training will you offer to airport IT staff and security administrators? • Will you conduct “train-the-trainer” sessions for operational teams?

Category	Key Questions
	• How will you ensure smooth handover for long-term system maintenance?
8. Implementation	• What is your plan for hypercare or post-go-live support? • What service-level agreements (SLAs) do you provide for response and resolution times? • How will you handle ongoing patches, updates, and version upgrades? • What is the escalation process for critical incidents or outages?
9. Maintenance & Vendor Support	• How will you ensure the system can handle seasonal peaks and large-scale events? • What monitoring tools or dashboards will be implemented for ongoing performance tracking? • How will the system scale to support future airport expansions or new regulations?
10. Cost & Budget Considerations	• What is the total cost estimate, including integration services, custom development, and maintenance? • What assumptions or exclusions should the airport be aware of? • How do you handle scope changes and associated cost impacts? • What are the key milestones for payment schedules?
11. Lessons Learned & Continuous Improvement	• What lessons have you learned from similar airport or large-scale IDMS projects? • Can you provide references from other airports or critical infrastructure clients? • What were the most common challenges in past projects and how were they overcome?

APPENDIX B: QUESTIONS FOR LEGAL ISSUES INTERVIEWS

1. Airports have used the following procurement methods for contracts for IDMS transfers.
    a. RFPs
    b. Sole Sources Contracts'
    c. Contracts with existing vendors (access control or consultants)

    Which tool did your airport choose and why?

2. Are you familiar with any other kind of procurement method or process that has been used? If, so, what was the method?

3. From the perspective of an airport seeking IDMS service transition, is there any procurement method your airports usually prefers? If so which one? If that's different from the one used for the IDMS transition, why was it chosen?

4. To the extent you are familiar with each of these procurement methods, what do you find the advantages and disadvantages of the following procurement methods?
    a. RFPS
    b. Sole Sources Contracts
    c. Contracts with existing vendors (access control or consultants)

5. In the absence of an RFP document, how did your airport establish contract requirements?

6. In negotiating contracts for a transfer of IDMS services, what do you view as the most critical issues or issues? Consider the following:
    a. Scope requirements
    b. Service levels
    c. Compliance issues
    d. Liability issues
    e. Insurance requirements
    f. Data control and security
    g. Indemnity
    h. Boilerplate contract language

7. What have you found to be the most contentious issues or the most difficult to negotiate? How did you resolve them?

8. What stakeholders do you see as most critical to the negotiation process in establishing a contract arrangement?

9. What is the role of a legal advisor in the process (on both sides)

10. What legal measures, if any, did you place into the contract to ensure cooperation from an incumbent IDMS provider being replaced?

11. How important is that cooperation?

12. Do you have any draft contract language addressing the following legal issues in your contract, that you think offers a model for contracts addressing IDMS transitions? Any language on the following topics?
    a. Service levels
    b. Compliance issues

c. Liability issues
d. Insurance requirements
e. Data control and security
f. Indemnity
g. Boilerplate contract language

13. What advice do you have for airports seeking to prepare contracts for transition of IDMS services?

14. What are the three best practices you can offer for such negotiations?

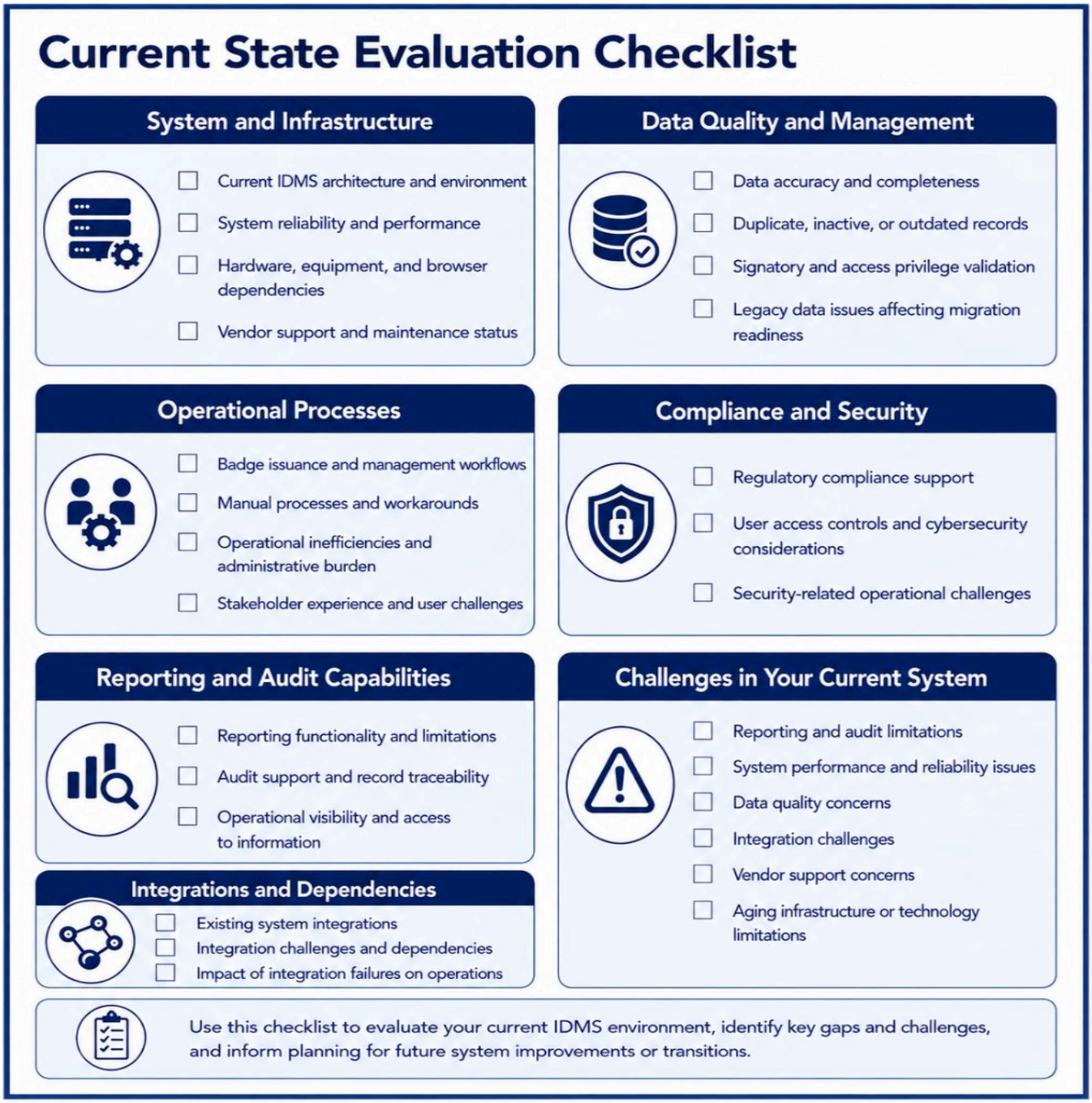
15. What are the three biggest pitfalls to avoid?

APPENDIX C: QUESTIONS FOR AIRPORT INTERVIEWS

Category	Key Questions
1. Project & Transition Planning	**Reasons for replacing IDMS:** 1. What are the reasons for replacing legacy IDMS? 2. How were those conclusions arrived at (user concerns, technical failures, cost increases, badge audits, reporting challenges etc.), 3. What are the key differentiators in the new IDMS vendor vs the legacy IDMS vendor and platforms? **Stakeholders**: 1. Who, what are the roles of the stakeholders in defining IDMS requirements, procurements and implementation and why?
2. Procurement	1. What are the additions or changes were included in the transition IDMS contract as result of lessons learned from the initial IDMS contract.
3. Environments, Data Migration & Integration	**Environments:** 1. How many environments (Dev, Test/ pre-Prod and Prod)? **Data Migration**: 1. What are the data sources (existing IDMS, ACS, DAC, CBT, other?) 2. Did the IDMS vendor perform the data migration OR was the airport IT involved with data migration process? 3. How was the data integrity and accuracy validated after migration (number of migrations) and where was the data migration performed (Dev or Test/Pre-prod)? **Integration**: 1. Other than the ACS, DAC, CBT did you have any other integrations? (new for transition or existing?) 2. Did you take advantage of the IDMS transition to change or improve integrations, badge layouts, badging office renovation and other processes. 3. Are there any custom APIs or middleware needed for legacy system integration and had to be maintained in the new IDMS?
4. Access Control & Security	**Access Control System:** 1. Keep existing or upgrade/ replace ACS. 2. If upgrade/ replace ACS, then the sequencing in reference to IDMS roll out. 3. Who performed the ACS upgrade/ replacement.
5. Compliance & Regulatory Considerations	1. Reporting (5%, ramp or other badge limits etc.) and Badge Audit 2. Is IDMS identified as critical system in CIP and what are the consideration within the CIP that you can share will be beneficial for other airports?
6. Operational Impact & Training	1. How were airport staff, tenants and other users trained on the new system? 2. Were there benefits / positives (learning curve, fundamentals of IDMS were known, workflow concepts were established etc.) when transitioning to new IDMS?

Category	Key Questions
7. Implementation	1. How were disruptions to daily airport operations minimized during the testing and cut over phases? 2. Does the IDMS vendor have remote access to Production systems? Or is it supervised remote access? 3. What local and federal requirements did you consider as you decommissioned the old IDMS system (data archive, server hardware etc.) to ensure privacy and security requirements are met?
8. Maintenance & Vendor Support	1. What is your maintenance and support program (duration, SLAs, liquidated damages, performance bond) with the IDMS vendor? Are these different from the legacy IDMS. 2. Do you have more robust cyber security requirements in the new IDMS than in the initial IDMS? What are the IDMS vendor responsibilities for reporting incidents (other airports), risk identification, mitigation planning etc.
9. Cost & Budget Considerations	1. What is the duration (period of performance) of the contract and what were the factors for the duration of the contract? 2. Were there unplanned / unexpected costs in implementation (customization, future upgrades, hardware requirements, integration licenses)?
10. Lessons Learned & Continuous Improvement	1. What are the most significant benefits and any limitations / challenges from the new IDMS solution? (key actions or processes, advice you would give to an airport, efficiencies in badge issuance, back-office functions).

APPENDIX D: CURRENT STATE EVALUATION CHECKLIST



APPENDIX E: DATA MIGRATION STRATEGY CHECKLIST



APPENDIX F: OPTIMIZED IDMS TRANSITION ROADMAP

