

IP/15 - ENHANCING CYBERSECURITY POSTURE FOR SINGAPORE AIR TRAFFIC MANAGEMENT AUTOMATION SYSTEM

02 June 2026



Presentation Overview

Importance of Cybersecurity

Cybersecurity is vital for protecting mission-critical Air Traffic Management systems from evolving cyber threats.

Cyber Threat Landscape

The cyber threat environment is increasingly complex, requiring robust and adaptive security measures for ATM systems.

Layered Security Approach

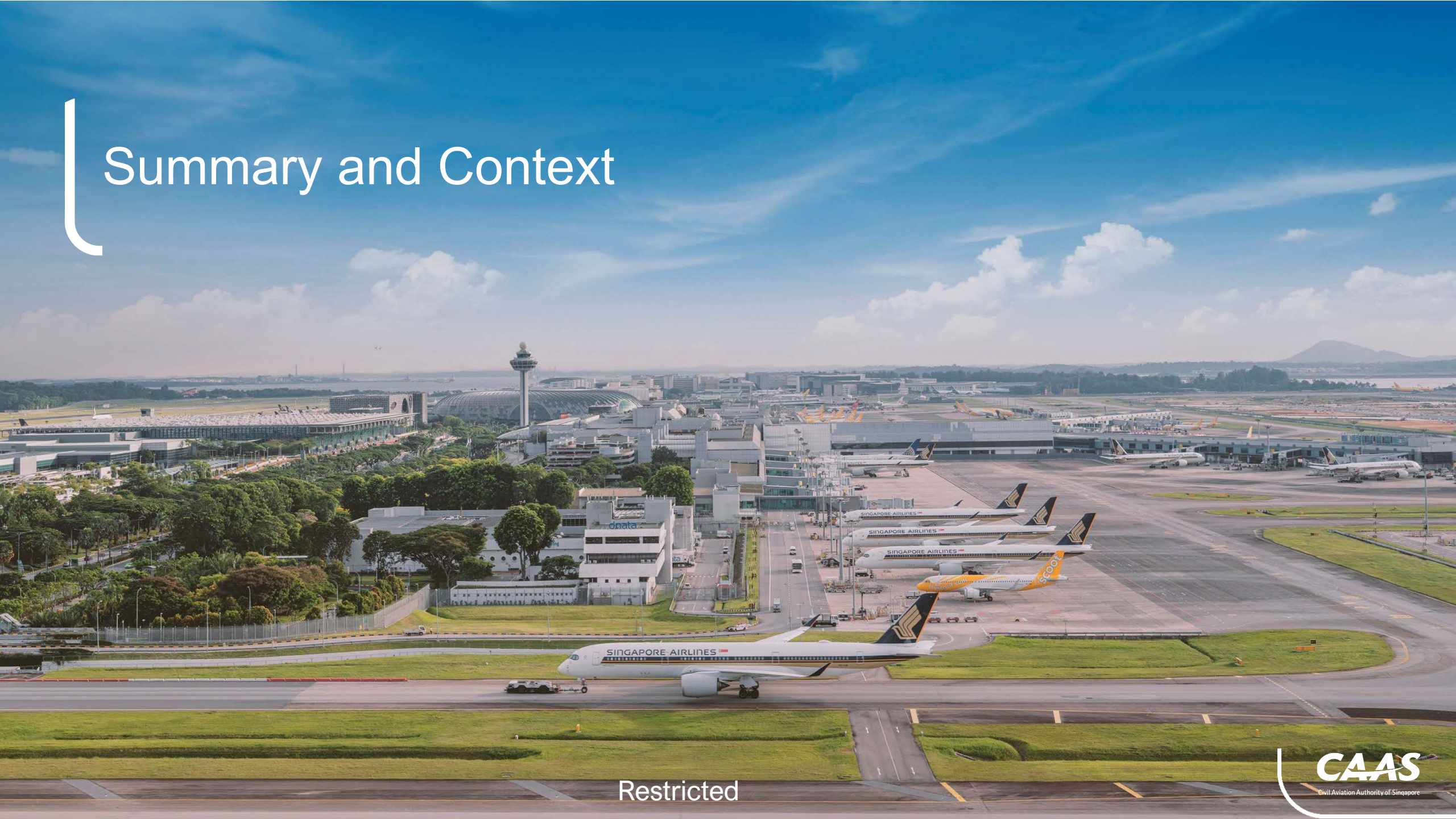
Singapore employs layered technical and procedural controls to enhance ATMAS cybersecurity resilience.

Managing Legacy Systems

Securing large-scale legacy ATM systems while ensuring continuous air traffic operations presents unique challenges.



Summary and Context



Restricted

Summary of Key Points

Singapore's Cybersecurity Approach

Singapore adopts a proactive strategy to enhance ATMAS cybersecurity against evolving threats and vulnerabilities.

Threats to ATM Systems

Mission-critical ATM systems face diverse risks from both external attackers and internal actors.

Layered Control Measures

Implementation of layered technical and procedural controls follows defense-in-depth to mitigate cybersecurity risks.

Challenges in System Upgrades

Upgrading and securing legacy ATM systems is complex, requiring continuous operation for safe air traffic management.



Overview of LORADS III



LORADS III Overview

LORADS III is Singapore's third-generation radar and display system managing air traffic within its flight region.

Data Integration

The system integrates surveillance data, flight plans, and communications for comprehensive air traffic management.

Safety and Cybersecurity

LORADS III is mission-critical, emphasizing the importance of robust cybersecurity for safe air traffic operations.

Importance of Cybersecurity and Risks



Restricted

Why Cybersecurity Matters for ATMAS

Increasing Cyber Threats

Cyber attacks on ATMAS are rising in frequency and sophistication, targeting critical safety and mission systems.

Expanded Connectivity Risks

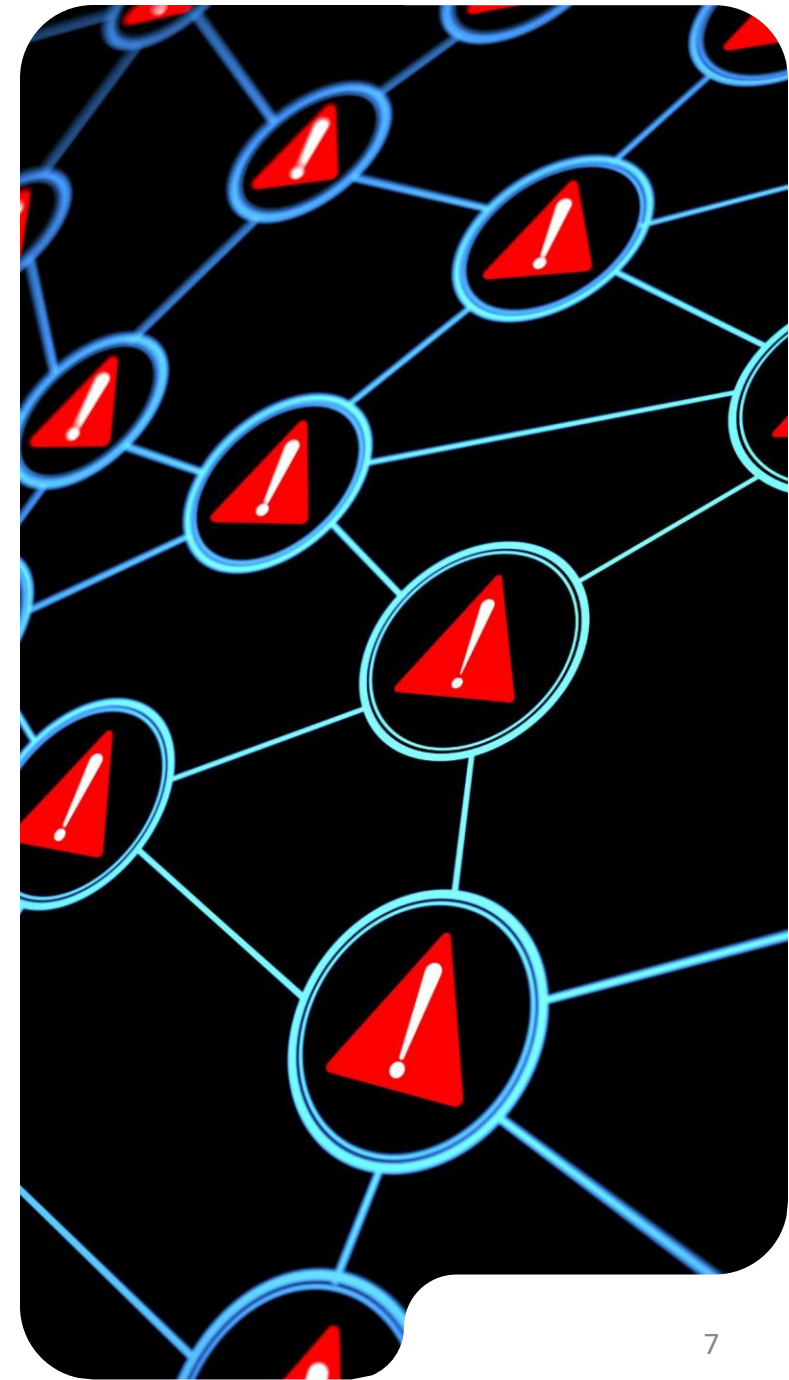
ATMAS connects with external private and public networks, increasing its exposure to cyber threats.

Operational Impact

Cyber incidents disrupting ATMAS could severely affect flight safety, airport operations, and airspace users.

Need for Resilience

Ensuring ATMAS resilience against cyber threats is essential for safe and continuous air traffic management.



Key Cybersecurity Risks

Advanced Persistent Threats

Well-resourced actors conduct targeted attacks disrupting or compromising ATM functions regularly.

Insider Threats

Malicious or inadvertent actions by authorized personnel pose significant cybersecurity risks.

Supply Chain Vulnerabilities

Malicious hardware or software can be introduced during procurement or maintenance activities.

Legacy System Risks

Outdated hardware and software with limited vendor support increase vulnerability to attacks.



Cybersecurity Controls and Assurance



Restricted

Layered Cybersecurity Controls



Defense-in-Depth Strategy

Layered cybersecurity controls follow defense-in-depth to prevent, detect, and respond to cyber threats effectively.

Access and Endpoint Security

Measures like Privileged Identity Management and Multi-Factor Authentication reduce risks of unauthorized access and malware.

Network and Monitoring Controls

Firewalls, network segmentation, and monitoring systems enhance visibility and restrict attacker movement within networks.

Cybersecurity Assurance Activities



Risk and Vulnerability Assessments

Regular risk and vulnerability assessments identify and address security weaknesses in systems.

Penetration Testing

Penetration testing simulates cyberattacks to uncover potential system vulnerabilities.

Configuration Reviews

Host configuration reviews ensure systems remain securely configured and compliant with security policies.

Cybersecurity Exercises

Cybersecurity exercises test incident response, disaster recovery, and business continuity plans.

Legacy Challenges and Upgrade Approach



Restricted

Challenges with Legacy ATMAS

Outdated Technology

Legacy hardware and software limit compatibility with modern cybersecurity solutions and require careful management.

Continuous Operation Constraints

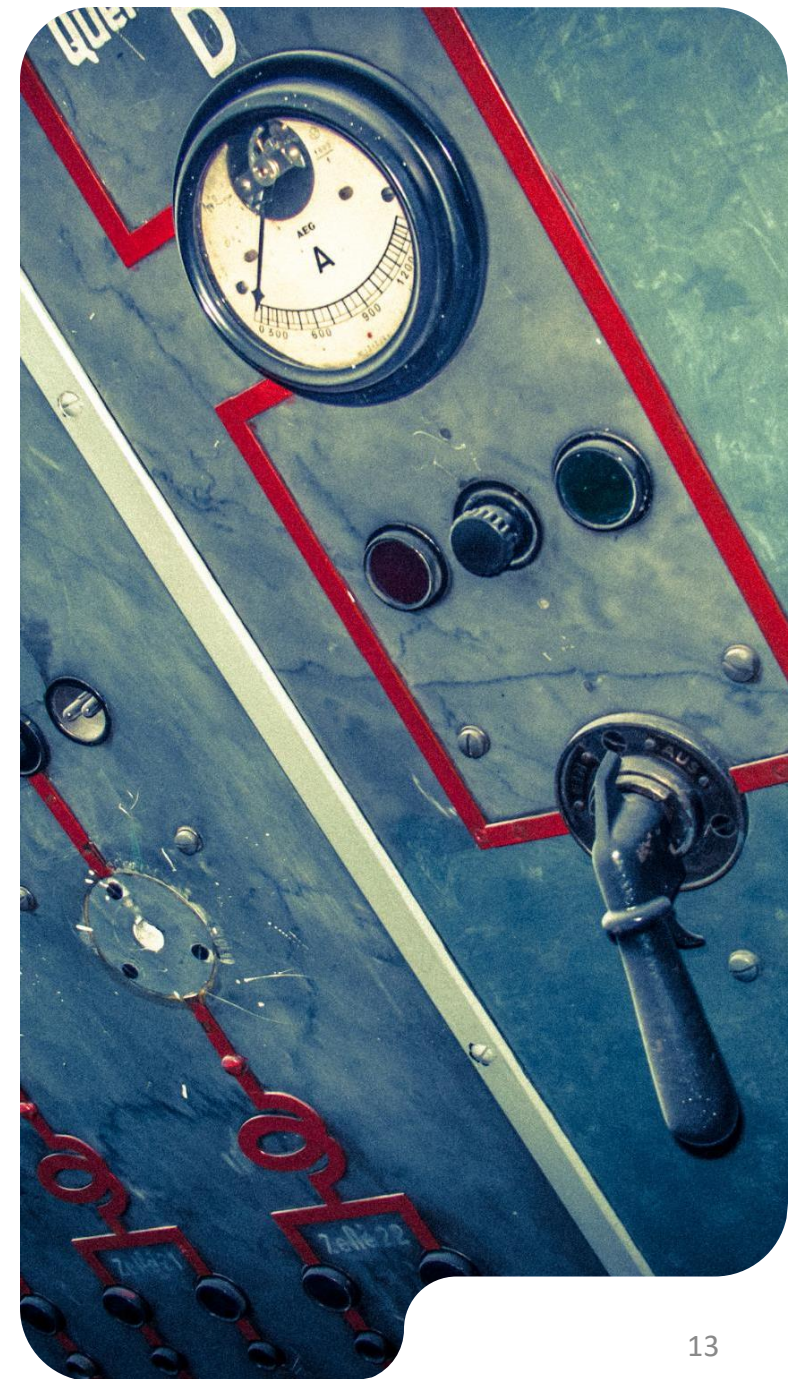
24/7 air traffic services restrict downtime for essential system upgrades and maintenance activities.

Integration Challenges

Compatibility issues hinder the incorporation of contemporary commercial cybersecurity tools into the legacy system.

Resource Limitations

Limited cybersecurity expertise and budget constraints affect the pace of system upgrades and protection measures.



Phased Upgrade Strategy and Integration

Phased Upgrade Approach

Singapore chose a step-by-step upgrade to minimize risks compared to a single large deployment.

Operating System and Application Upgrade

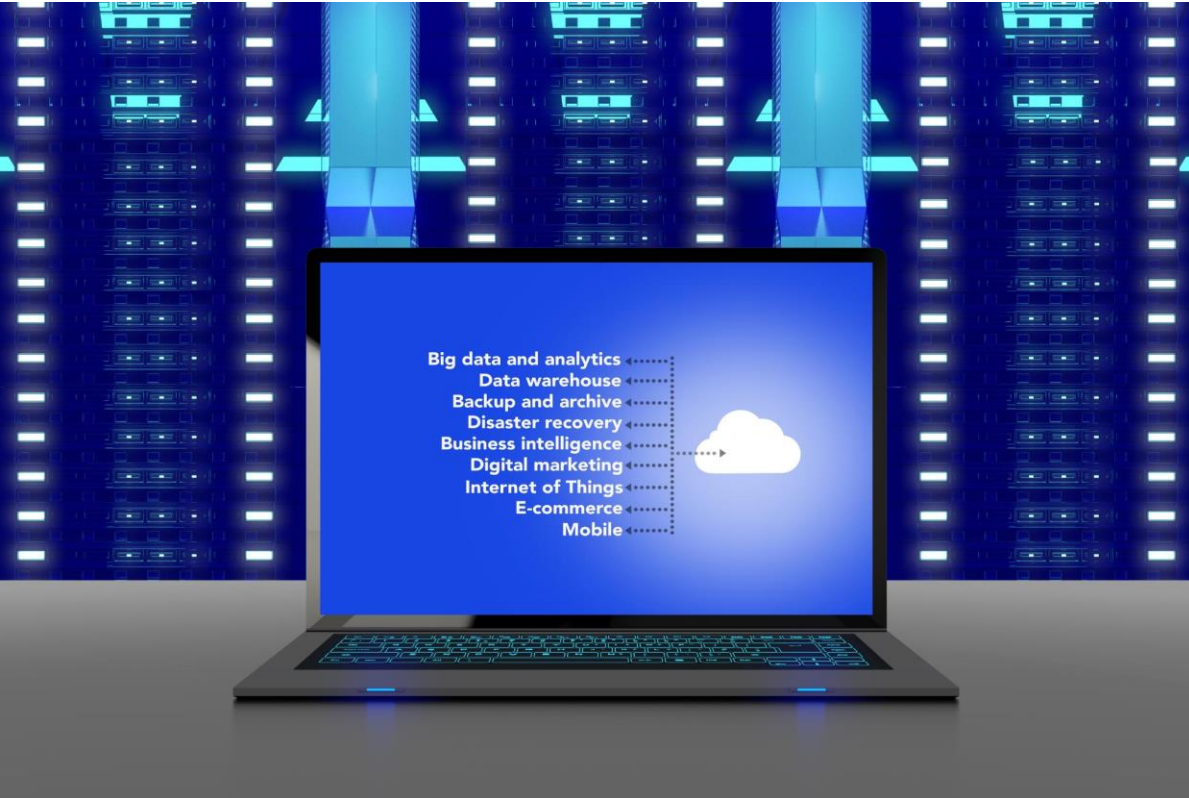
The first phase included OS upgrades, hardware improvements, and porting to 64-bit systems with dual-boot for smooth transitions.

System Monitoring and Cybersecurity Integration

Second phase migrates to new monitoring and cybersecurity subsystems with incremental onboarding of security features.

Careful Monitoring and Integrity

Each upgrade phase is carefully monitored to maintain system performance and operational integrity.



Conclusion and Action



Restricted

Key Takeaways



Cybersecurity Importance

Cybersecurity is essential for the safety, resilience, and continuity of ATMAS operations in air traffic management.

Threat Landscape and Controls

Evolving threats require ongoing risk assessments and layered defence-in-depth strategies to mitigate risks effectively.

Legacy System Security

Securing legacy ATM systems needs phased planning and coordination to minimize impact on air traffic services.

Incremental Upgrades and Assurance

Singapore's experience shows that incremental upgrades and strong assurance improve cybersecurity while maintaining operations.



For Discussion

The End



Restricted