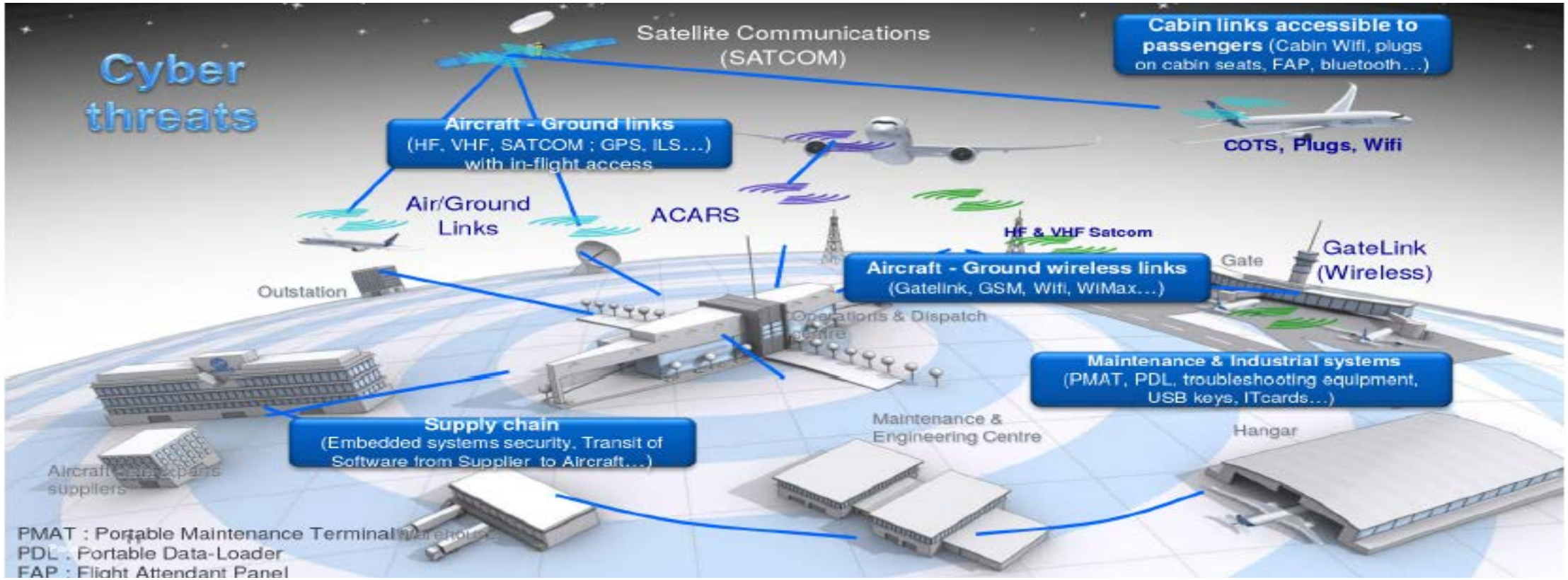
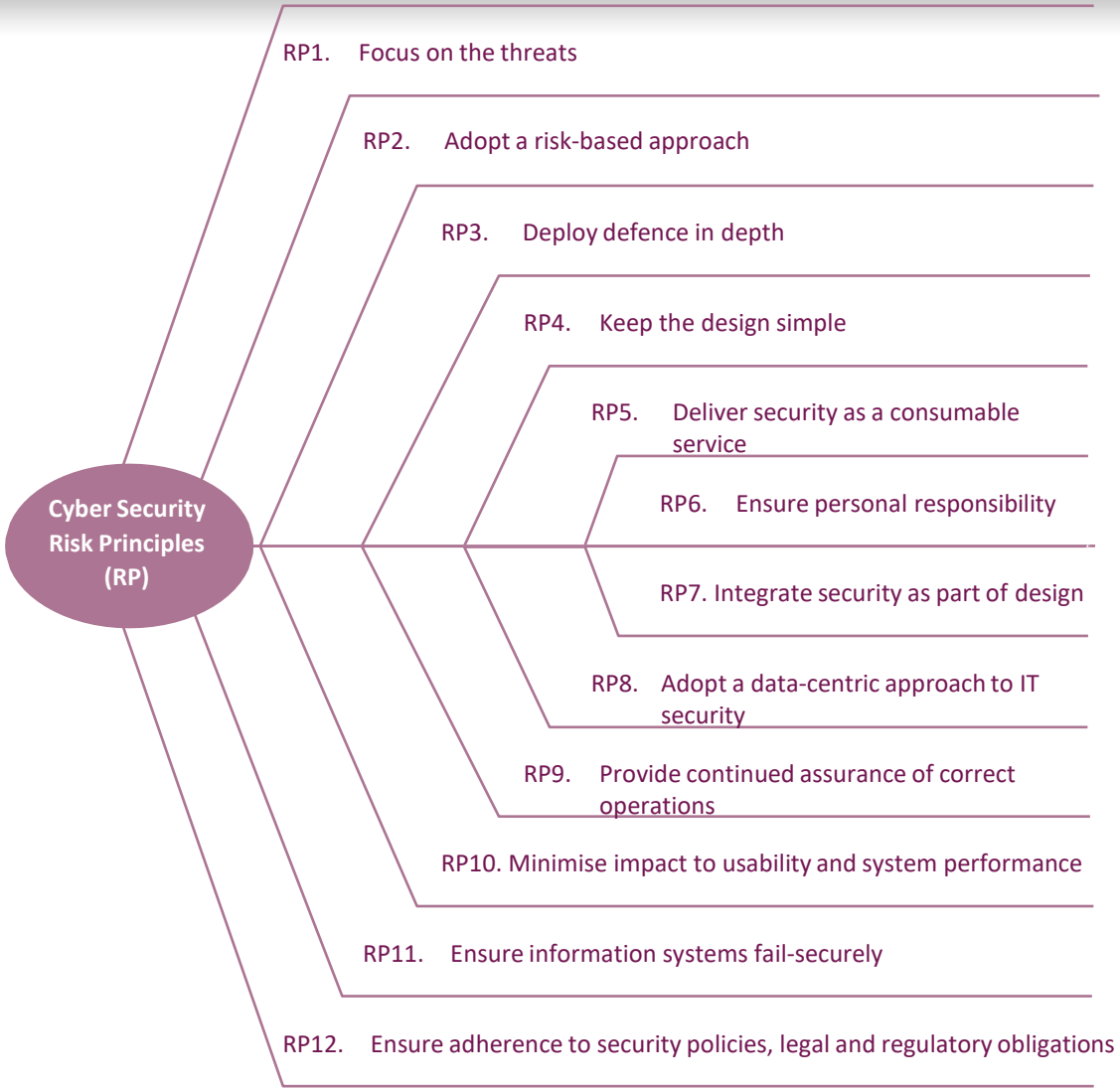
Aviation Cybersecurity Framework: to enhance the resilience of aviation infrastructure against cyber threats

Farhan Chaudhry, VP Cyber Security, Governance, Risk and Compliance & Aircraft Cyber Security

Qatar Airways Group

Aviation / Aircraft Cybersecurity Threat Landscape





RP1: Threats should be understood and documented, including how they are prevented, detected or responded to

RP2: Protection measures should be appropriate to the degree of risk present

RP3: Multiple layers of security should be implemented to mitigate the possible failure of one security component

RP4: The design of an information system must be kept as simple as possible

RP5: Protection measures should be designed to be consumed as common security services

RP6: Users of an information system must be aware of their personal responsibilities to prevent unauthorised access to, and compromise or theft of, information assets and systems

RP7: Security should be treated as an integral part of the overall system design

RP8: Data should be secured end-to-end throughout its lifecycle

RP9: Provide assurance that the information system is, and will continue to be, resilient in the face of (un)expected threats

RP10: The impact of security protections on users and systems should be considered

RP11: In the event of a failure, an information system should fail into a secure state

RP12: The development, build and deployment of systems should be consistent with defined information security policies. legal and regulatory obligations

Framework Development – Establish the Foundations

6. Aircraft Cyber Security Program

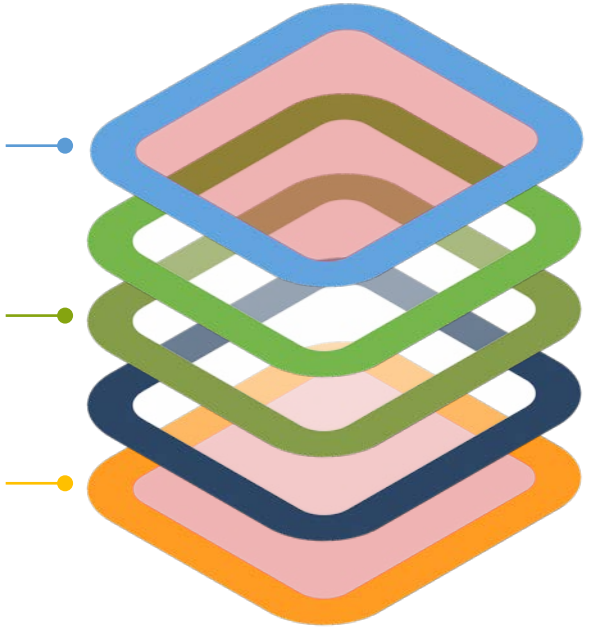
Establish the plan to mitigate the vulnerabilities identified from the previous activities.

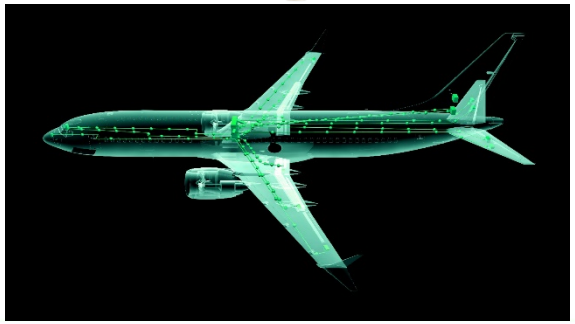
4. Security Log Review

Assess monitoring and detection capabilities

2. Technical Risk Assessment

Technical Security Assessment and / or pentests should be performed during cyber security risk assessment.





5. Training & Awareness

Develop capabilities and asset management foundations to manage and monitor risk assessment findings.

3. Aircraft security handbook

Ensure compliance to security handbooks

1. Security Risk Assessment

Execute an identification and assessment of risks related to cyber-attacks based on Threat Vectors and Industry standards e.g. NIST (Special Publication 800-30).

The value drivers of an effective Aircraft Cyber Security Risk Framework are important enablers

Define a set of strategic imperatives…

Reduce Operational Risk
Highly secure systems, resilient and scalable systems, operations workflow improvements, releasing quality change quickly but securely

Ensure Compliance with Regulation
Large effort to conform to new regulations, enhanced fraud detection and prevention solutions, quality reporting data to regulators, integrated real-time quality MI reporting to Operations users

Improve Efficiency
Optimise IT infrastructure and IT service, simplify IT estate and right-size IT operations and development teams with effective governance of processes

Increase Opportunities with effective processes
Test and drive incident and crisis planning. Drive automation, and effective outcomes. Focus on integrated customer experience, explore performance metrics

…and develop risk based framework to be a key enabler

- **Scalability** through autoscaling of the technology estate to respond to Resiliency Demands
- **Highly resilient and secure** architecture with multiple availability zones, advanced DDoS protection and firewall technology
- **Rapid and incremental releases** minimising the delivery risk of large scale releases and upgrades
- **Test Connectivity** to reduce manual effort and limit human errors, driving secure solutions

- **Compliance as a foundation** ensure all standards are reviewed for compliance into deployments from the outset
- **Reporting and Oversight** to notify of compliance issues and breaches
- **Leverage** technology to query large volumes of data and find patterns to detect deviation cases or reporting anomalies
- **Easily verify regulatory changes** by deploying baseline standards

- **Automated Application and Software rightsizing** to optimise the technology estate and reduce cost
- **Optimisation mindset** can be leveraged to drive playbooks and runbooks

- **Rapid and safe product development** in sandboxed environments to trial and build new and innovative product offerings
- **Powerful Cloud based analytics** technology to analyse new opportunities and products to provide highly targeted customer experiences
- **Plug and play models** to facilitate experimentation of AI and new tools and bi-directional sharing of data in a controlled manner
- **Enhanced Data Security** enforce Multi Step and Factor Authentication for PII data related activities

THANK YOU