الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY

وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS

Aviation Cyber Security Guidelines

Aviation Cyber Security Guidelines

Issued By:
Civil Aviation Authority and Ministry of Transport & Communications

Issued On: April 2019

Contents

Disclaimer

This document is intended to provide guidelines to the aviation sector on addressing cyber security risks.

While every care has been taken in the preparation of the document, the threats scenario is changing constantly. Organizations are expected to use this document as a foundation and ensure that its recommendations are implemented as baseline requirements.

Target audience identified within this document need to ensure that the guidelines are incorporated within their overall information security program,

Copyright

Acronyms and Abbreviations

ACARS	**Aircraft Communications Addressing and Reporting System**
ADS-B	Automatic Dependent Surveillance — Broadcast
ASDE	Airport Surface Detection Equipment (surface movement radar)
AeroMACS (WIMAX Based)	Aeronautical Mobile Airport Communication System
CC	Common Criteria
CSP	Certificate Service Provider
DCS	Departure Control Systems
EAL	Evaluation Assurance Level
FIS-B	Flight Information System-Broadcast
FIS-B	Flight Information System-Broadcast
GNSS	Global Navigation Satellite System
IFE	In Flight Entertainment
RNP	Required navigation performance
RPO	Recovery Process Objective
RTO	Recovery Time Objective
SWIM	System Wide Information Management
TIS-B	Traffic Information Service – Broadcast
TLP	Traffic Light Protocol

Definitions

Eavesdropping	The act of listening in to the unsecured broadcast transmissions
Jamming Attack	The ability to effectively disable a single node (both ground stations or aircraft) or an area with multiple participants from sending/receiving messages by an adversary.
Message Injection	The ability to inject non-legitimate messages into the air-traffic communication system.
Message Deletion	The ability to physically "delete" a message from the wireless medium by utilizing destructive or constructive interference.
Message Modification	The ability to manipulate an original legitimate message in an air-traffic communication system.
Recovery Point Objective	The recovery time objective is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity
Recovery Time Objective	A recovery point objective is the maximum targeted period in which data might be lost from an IT service due to a major incident.

1. Introduction

Qatar is at the cross roads of a very challenging time in its history, making efforts to become a developed economy playing a crucial and responsible role in global politics. Fueled by the ambitions set within the Qatar 2030 vision by its leaders, it is imperative that various sectors within its society and economy work together to build a resilient nation.

The Aviation industry is one of the corner-stones in realizing this dream. It is a critical service, enabling the nation to connect to the rest of the world. A significant population of the country are expatriates who live in Qatar to make a living. A strong aviation network ensures its residents can enjoy stress-free travel to their homelands and back. The Air Cargo service ensures that the best goods produced globally are available in Qatar including fresh farm produce. It also plays an important role in transporting manpower to and from remote oil fields and ensuring quality and prompt emergency medical / ambulance services.

However, the aviation industry, known for its safety and reliability, is quickly moving on to embracing technology at a fast pace. Comforts, hitherto unheard of, are now a reality. Telecom connectivity, internet access, Bring Your Own Entertainment are now available in the skies during air travel. Along with the comforts it brings to its customers, this technology introduces a new set of risks that needs to be managed to ensure that the safety and reliability of the aviation sector is not compromised.

Globally a number of organizations are now working towards producing standards and guidelines to protect the Cyber security posture of the aviation sector.

The Civil Aviation Authority (Qatar) along with the Cyber Security Division of Ministry of Transport and Communications would like to take a step further in this direction and provide cyber security guidance to this critical sector in Qatar.

These guidelines will assist operators and stakeholders within the aviation sector to improve their cyber security posture and build a resilient organization.

2. Legal Basis

The Qatar Civil Aviation Authority (QCAA) was established under Article 4 of the Emiri Decree No. 16 of 2001.The QCAA is the designated authority for aviation security within the state of Qatar. The Chairman of QCAA has been vested with powers to issue regulations, through articles 04,11and 24 of Law No. 15 of 2002.

1. The Primary Legislation under Law No. 15 of 2002
2. Law No. 3 of 2011 which amends Law No. 15
3. The Civil Aviation Security Quality Control Regulation of 2010.
4. The National Civil Aviation Security Programme (NCASP)
5. Chairman's Decree no. 6 of 2015 (Hamad International Airport User Regulation)
6. Chairman's Decree no. 10 of 2015 (Restricted Area Regulation)

Primary Legislation under Law no. 15 of 2002:

The terms and provisions of these Conventions are given legal force in Qatar by virtue of Law No. 15 of 2002 which is the primary law of Civil Aviation, through the following articles:

Articles 94 and 95	Lists acts considered as offences regarding violence onboard the aircraft and destruction of navigational facilities and also explains the Jurisdiction.
Articles 99 and 100	Limit of responsibility for the compensation and arrest.
Articles 103, 106, 107 and 108	Penalties for aviation related offences.

3. Scope and Audience

Cyber security comprises of controls (covering people, process and technology) designed to protect systems, networks and data[1] from digital attacks.

The cyber security guidelines prescribed in this document cover critical information systems within the aviation eco-system[2]. These include but are not limited to:

1. Air Traffic Control Systems
2. Airport Operators (QAS and or any other entity who uses a DCS / BRS or airline reservation system)
3. Airport Information Systems
4. Aircraft operators (Local / National / Foreign carriers operating in Qatar)
5. Aircraft Systems
6. Airport Tenants (e.g. QAS Cargo, QACC, QDF etc.)

The intended audience for this documents includes stakeholders[3] that manage the critical information systems within the aviation eco-system.

These includes

1. Air Traffic Control operators that manage communication with airplanes during flight / landing.
2. Airport Authorities / Operators who manage critical information systems at the airports. This includes Passenger Information Systems, Airport Information System, Baggage Handling systems etc.
3. Information Systems within an airplane including its communication systems, flight entertainment systems, internal controls etc…

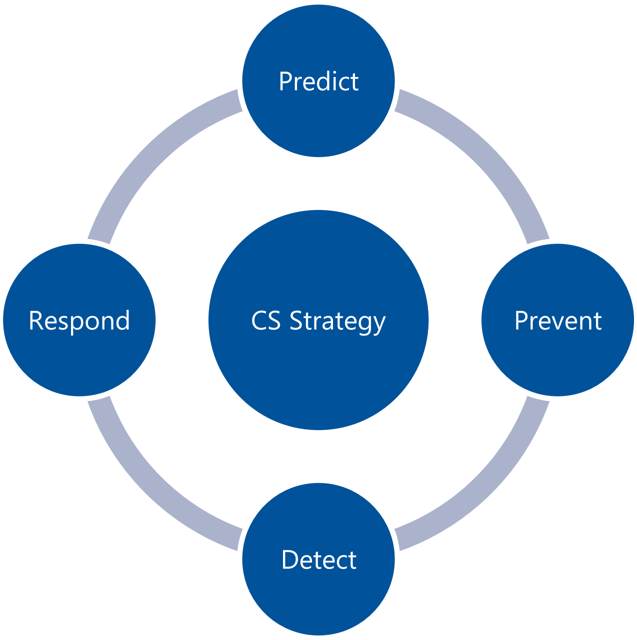
[1] Systems, Networks and Data here collectively refer to corporate information systems, business information systems, industrial control systems, IoT etc.

[2] The document scope includes only commercial and civil airlines, licensed and managed by CAA. Any Military / Defense systems are out of the scope of this document.

[3] Stakeholders include the system owner, its staff, contracted third party staff that is part of the operations, vendor and their staff supporting the critical information systems.

4. Overall Strategy

A key to managing cyber security risks within the aviation sector is to develop a 360 degree approach, a comprehensive strategy capable of predicting cyber risks to the aviation ecosystem, identifying and implementing suitable controls to prevent cyber risks, the capability to monitor / detect attacks and the ability to respond and recover from successful attacks.[4]



Predict: "Predictive" capabilities enable the security organization to learn from external events via external monitoring of the hacker underground to proactively anticipate new attack types against the current state of systems and information that it is protecting, and to proactively prioritize and address exposures. This intelligence is then used to feed back into the preventive and detective capabilities, thus closing the loop on the entire process.

Prevent: "Preventive" strategies include policies, products and processes that are put in place to prevent a successful attack. The key goal of this category is to raise the bar for attackers by reducing their surface area for attack, and by blocking them and their attack methods before they impact the enterprise.

Detect: "Detective" capabilities are designed to find attacks that have evaded the preventive category. The key goal of this category is to reduce the dwell time of threats and, thus, the potential damage they can cause. Detection capabilities are critical because the enterprise must assume that it is already compromised.

Respond: "Responsive" functions are required to investigate and remediate issues discovered by detective activities (or by outside services), to provide forensic analysis and root cause analysis, and to recommend new preventive measures to avoid future incidents.

[4] Based on Gartner's Cyber Security Strategy Model

5. Risks and the Evolving Threat Landscape

5.1. Identifying Cyber Security Risks to the Aviation Sector

To understand cyber security risks to the aviation sector, we need to understand risks and the factors that influence it.

The following is an attempt to present risk in a simplified manner to set the context. Agencies can refer to the multitude of information available on the subject. They could also refer to the Qatar IT Risk Framework and / or the IATA's Risk Framework.

By definition:

Assets is something that an agency would like to protect and covers People, property, and information. **People** may include human stakeholders such as employees, customers, contractors or guests. **Property** assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. **Information** may include databases, software code, critical company records, and many other intangible items.

Threat is anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Vulnerability is a weakness or gap in a security program that can be exploited by threats to gain unauthorized access to an asset.

Summing it up, **IT Risk** is defined as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the agency. It is measured in terms of a combination of the probability of occurrence of an event and its consequence.

Risk is a function of threats exploiting vulnerabilities to obtain, damage or destroy assets. Thus, threats (actual, conceptual, or inherent) may exist, but if there are no vulnerabilities then there is little/no risk. Similarly, you can have a vulnerability, but if you have no threat, then you have little/no risk.

Accurately assessing threats and identifying vulnerabilities is critical to identifying cyber security risks within the aviation sector. A proper security framework should include the following objectives:

1. Understand the risk and nature of the threats
2. Conduct research and development
3. Communicate the risk and ensure situational awareness
4. Take necessary measures to strengthen the defense system and design mitigation strategies
5. Ensure the industry and government are working together to keep threats at bay

Since aviation is deeply rooted in safety, there are two additional factors that security practitioners in the domain should look into carefully:

1. **Black Swan Event:** The Black Swan, is defined as an extreme event that have the following three key characteristics:
    a. Their probability is low, based on past knowledge and experience.
    b. Although probability is low, when it happens it has a devastating impact and the shock caused is profound.
    c. It is impossible to predict the exact nature of the event, but they are retrospectively defined as an event of obvious concern and should or could have been better understood and, to some degree, forecast as a potential risk.

    Furthermore, black swans could be compounded by the simultaneous occurrence of risk events, perhaps due to undetermined or flawed assumptions. E.g. Tsunami followed by an earthquake.

2. **Risk Velocity:** Risk Velocity is an indication on how soon the effects of risk will be felt. The table below outlines how the velocity of a risk could be assessed in a qualitative manner.

Velocity Measure	**High**	**Medium**	**Low**
Time to Impact	Risk impact will be felt in less than a week after occurrence	Risk impact will be felt in between a week to a month after occurrence	Risk impact will be felt more than a month after occurrence
Reaction Time	There will be very little or no time for reaction and response planning before serious consequences of the risk hit	There will be limited time for reaction and response planning before serious consequences of the risk hit	There will be time for reaction and response planning before the serious consequences of the risk hit

5.2. Evolving Threats

The aviation sector is deeply rooted in the principle of safety, however the past few decades has seen technology make huge strides and inroads into the aviation sector. The technology on one hand has revolutionized the travel making it easier to travel non-stop across continents, providing facilities to air passengers like never before (Internet access, GSM access, In-Flight entertainment), seamless transfers for passengers transiting between countries, but on the other hand these comfort have not come without its set of risk that have surfaced on account of the inherent vulnerabilities and known threats that these systems possess.

The usage of onboard and off-board computer systems, navigation systems and prevalent use of data networks, has led to increased threats about cyber-attacks and data breaches.

The following are some of the leading threats faced by the aviation sector:

Phishing attacks: Phishing attacks is primarily a pre-step to a full blown targeted malicious attack towards an organization. The primary objective being to gain user credentials through social engineering techniques and infiltrate an agency's system to plant and launch advanced persistent threats. A number of organizations including airports have been victim of such attacks.

WiFi-based attacks: Unless secured adequately, traditional Wi-Fi systems available onboard in an aircraft are vulnerable and malicious actors could use them to possibly breach into on-board avionics equipment and disrupt or modify satellite communications. A framework of code injected by malicious actors could probably get into the plane's system and override security implementations leading to disastrous potentialities such as hijacking and / or mid-air crash etc.

BYOD: Current in-flight entertainment systems allow the passengers to watch their own videos by way of USBs. Unless adequately protected, the malicious actors could potentially use the USBs to inject malicious programs / APTs in to the in-flight entertainment systems with disastrous consequences. For e.g. the flight information provided on the IFE could be falsified or distorted to create chaos / panic amongst the passengers.

DDoS and botnet attacks: Distributed-denial-of-service attacks have grown in popularity to carry out a range of malware injection activities. Within such attacks, hackers utilize botnets of compromised networks to flood air traffic control and other critical systems (e.g. online ticket booking) with traffic, which results in a crash of the platform. Attackers may also ask for a ransom amount from the authorities to prevent disruption of flight management and control systems.

Jamming attacks: The attack can have dire consequences as the hackers compromise the accuracy of data provided to the aircraft management, such as speed, location and direction of nearby airports and other planes.

Remote hijacking: Security flaws in communication technologies utilized in the aviation industry enables hackers to remotely attack/control in flight and on-board systems which in turn could open a gateway for malicious actors to attack other critical systems such as flight controls, engine and fuel systems, navigation receivers, surveillance systems, aircraft displays, and others.

Ensuring secured aviation systems and staying ahead of these threats requires the aviation industry to collaborate with manufacturers, governments, airlines and airports. It is also important for the sector to establish a cyber security culture and develop mitigation/prevention strategies after threat analysis.

5.3. Threat Actors

Risk Assessment is the probability of threat being realized, however a key factor to be considered is the Threat Actor and his capability to execute the threat. E.g. DDoS is a threat to information systems infrastructure, but a successful execution of this threat depends on who is executing this threat i.e. is it a script kiddie, hacktivists or state actors.

A sample list of threat agents and their probable rating is provided in **Appendix D**

6. Intelligence Gathering and Sharing

Sectors that are critical to the wellbeing of a nation and the organizations that operate within (Critical Sector Organizations (CSO)) are under constant threat. It is imperative that such sectors (CSOs and their regulators) implement prudent and pragmatic threat monitoring mechanisms. A highly recommended practice is to be able to share threat intelligence within the sector i.e. between the CSOs in a sector and the regulator. This will enable each entity to leverage upon the capabilities of other and produce a multiplying effect.

Nevertheless, traditionally, information sharing has been an itchy matter both between peers within a sector and with the regulator themselves. However, it is important that we look beyond and put in place a governance structure that provides assurance to its members to be able to share threat information with each other.

Information sharing can happen in one of the following ways:

Information Disclosure: Regulators can enforce their stakeholders to disclose certain information to them by way of regulations. This could include annual reports, information about cyber incidents, malicious attacks etc. The frequency could be fixed or ad-hoc based on a trigger. Regulators could then choose to make public the information shared or parts of it based on the need and in line with the agreed information sharing agreement.

Information Sharing Groups: CSOs within a sector could come together with or without the regulator and mutually agree amongst themselves to share information (specific information agreed between the group) within an agreed framework.

When evaluating potential sharing partners, an agency should look to sources that complement its existing threat information resources or that offer actionable information that addresses known gaps in an agency's situational awareness. Since sharing communities may focus on the exchange of a specific type of threat information, an organization may need to participate in multiple information sharing forums to meet its information sharing objectives.

6.1. Information Disclosure

Agencies responsible for managing and / or operating airports, aircrafts or any associated critical systems such as Air Traffic Control should disclose information relating to cyber-attacks (attempted or successful) on its systems to identify and address the vulnerabilities to Qatari commercial aviation system.

The following guidance may be used in determining the frequency for sharing the information with the designated agencies.

Criteria	Description	Recommended Frequency
Critical	A successful breach or compromise on a critical system within the agency / crippling DDoS attacks A breach within a non-critical system (e.g. corporate systems) but which impacts the operations of the agency. A targeted attack on the Agency's critical systems	0 – 2 hours
High	A targeted attack on the agency and / or its systems / Huge DDoS attacks A breach within a non-critical system but which has the possibility / potential of impacting the critical systems or the operations of the agency	2-8 hours
Medium	Potential attacks / DDoS attacks / Website defacements etc	Summarized as part of the Annual report
Low	Low intensity attacks, malware infections etc	Summarized as part of the Annual report
Annual	Summary of all attacks, with focus on Critical and High categories	

The information disclosure shall be done to the following authorities in a prescribed format. A template for the same can be found at **Appendix B**

1. Civil Aviation Authority
2. Q-CERT, Ministry of Transport and Communication

6.2. Information Sharing Group (ISG)

CAA / MOTC can facilitate establishment of an Information Sharing Group for the aviation sector. The membership will comprise of members from CAA, MOTC (Cyber Security), ATC, Airlines and Airport operators.

The ISG should formulate procedures that allow sharing of threat information while at the same time satisfying the concerned agency's obligations towards protecting potentially sensitive data.

The procedures should,

1. To the extent possible, balance the risks of possibly ineffective sharing against the risks of possibly flawed protection.
2. Describe the roles, responsibilities, and authorities (both scope and duration) of all stakeholders.

3. Allow for the effective flow of shared information to members. Traffic Light Protocol (TLP) is a commonly accepted protocol for sharing information in such groups. **Appendix G** provides additional information.
4. Enable collaboration with approved external communities when needed.

Agencies desirous of participating in ISGs should obtain approval from the:

1. Leadership team that has oversight for information sharing activities and for controlling the resources necessary to support the organization's information sharing goals;
2. Legal team or those with the authority to enter into commitments; and
3. Privacy officers and other key stakeholders that have a role in the collection, ingest, storage, analysis, publication, or protection of threat information.

Agencies desirous of participating in ISGs should ensure adequate information sharing and tracking procedures that include:

1. Identification of threat information that can be readily shared with trusted parties.
2. Describing the conditions and circumstances when sharing is permitted
3. Established processes for reviewing, sanitizing, and protecting threat information that is likely to contain sensitive information.
4. Identification of approved recipients of threat information.
5. Plans for addressing leakage of sensitive data.
6. Automating the processing and exchange of threat information where possible.
7. Process for handling non-attributed information exchange, when needed.
8. Tracking internal and external sources of threat information.
9. Information handling designations that describe recipient obligations for protecting information.

An organization's information sharing rules should be reevaluated on a regular basis. Some of the events that can trigger reevaluation are:

1. Changes to regulatory or legal requirements,
2. Updates to organizational policy,
3. Introduction of new information sources,
4. Risk tolerance changes, Information ownership changes,
5. Changes in the operating/threat environment, and
6. Organizational mergers and acquisitions.

7. People and Process Controls

7.1. Establishing Leadership and Governance

Establishing leadership for the information security program within the organization is very important. It has been duly emphasized in all security standards as well as the National Information Assurance Policy.

This is all the more important and complicated in the aviation sector within Qatar and countries that have similar models. For example, Qatar Airways as the incumbent player not only operates the airlines but also through its subsidiaries manages the airport services, commercial duty-free shopping services, hotels, catering etc.

7.1.1. Leadership

It is important to identify who "owns" cyber security in such a scenario. The answer is complex and highly dependent on the airline's structure and preferred approach to technology.

The organization should establish a leadership for the information security program. The right accountabilities and responsibilities should be assigned within the organization.

The organization may choose a hierarchical model that may assign leadership roles for independent business unit or profit centers with a single person at the top that oversees and is responsible for the complete information security program to the board.

Further, define a RACI matrix that clearly identifies and assigns information security roles for the various business units and critical systems within the organization. Below is a proposed template that organizations may use or customize based on their organization structure.

RACI Table for representing Information Security roles and assignments

Business Unit / Systems	Board of Directors	CEO	Sr. Management (Business)	CIO	CISO	Risk / ERM	Legal	BU InfoSec Lead	IT OP Team	Sec OP Team
Airline / Aircraft Operator										
Avionics (e.g. QR)										
In Flight Communication Systems										
In Flight Entertainment Systems										
Airport Operator										
Information Displays (e.g. QAS)										
Passenger Check In										
Baggage Handling Systems										

Air Traffic Control										
ATC Systems										
Radar / Communication Systems										
Supply Chain System										
Aircraft Manufacturer										
Systems Suppliers										

7.1.2. Governance

Each organization should develop a comprehensive framework of Information Security and Privacy policies and procedures to effectively implement and manage the enterprise information security / privacy management system.

The framework must include a Corporate Information Security Policy (CISP)[5] outlining the organizations commitment to adopt information security / privacy practices within the business and to implement an effective management system to deliver the objectives. The Head of the organization must sign the policy.

A policy manual covering various processes and specific domain areas should complement the CISP.

7.1.3. Legislations

The management system and the associated policy manual should define controls in line with regulatory requirements. The regulatory requirements include local as well as international (where applicable) requirements.

Some of the key regulatory requirements include:

1. Adherence to National Information Assurance Policy (Qatar)
2. Adherence to Personal Information Privacy Protection Law (Qatar)
3. Adherence to Cyber Crime Law (Qatar)
4. Adherence to Cybersecurity guidelines and recommendations issued by Qatar Civil Aviation Authority
5. Adherence to ICAO Cybersecurity recommendations.
6. Adherence to IATA Cybersecurity recommendations.
7. Adherence to GDPR
8. Adherence to any other country specific regulations where the businesses operate.

[5] http://www.qcert.org/sites/default/files/public/documents/cs-csps_template_for_corporate_information_security_policy_v2.1.docx

7.2. Securing the Humans

Humans form the weakest link in the triad of "People, Process and Technology" that is used to build any effective management system including for information security. However, Humans are the most important element, because the process and the technology are dependent on it. In a way to a certain extent the process and technology will be designed, implemented and operated by humans.

As such it is imperative that humans are effectively educated about the cyber threats and ways to mitigate them through the use of acceptable good practices. Within the context of an organization, "humans" would include employees, outsourced staff, contractors, vendors, customers, board members and shareholders.

Cyber education for human is primarily driven through Awareness and Training. Cyber education is critical to ensure that the human element is aware and about cyber threats.

7.2.1. Awareness

In general, awareness is about creating an alert mind that is able to detect, react and inform when a cyber threat occurs.

Security awareness sensitizes the human elements against cyber threats, teaches good practices to manage these threats and communicate (escalate) the threats detected to the concerned stakeholders.

Security Awareness should be provided to all relevant stakeholders within the organization. However, the message and the tone should be customized to the relevant groups to ensure that the intent and the essence is communicated well and accepted by the intended audience.

NIA Policy Section B-7 Security Awareness covers in details the elements of a security awareness program.

Appendix H provides guidance on awareness around aviation security as prescribed by ICAO.

7.2.2. Training

Training by definition is a specific knowledge imparted to build / raise the skills of a person. It is provided to a select group of people identified within an organization and delegated with the responsibility of carrying out a particular task.

Cyber security is a dynamic field, everyday new threats are discovered, technology is changing at a very rapid pace, the information perimeter of an organization is virtually nonexistent today, as such it is important that the team tasked with the responsibility of securing the organization's information assets are abreast of this volatility and have the requisite skillsets to manage them.

This can only be achieved by way of a structured training program that will ensure that the organization has the right skill sets in terms of quality and quantity to protect its information assets.

The information security skills development program should be managed jointly by the Cyber-security leader within the organization, the Human Resources Manager (Department) and the Training Manager (Department) and should include:

1. An updated skills matrix developed at an organization level to assess the available skills within an organization.
2. An annual GAP Analysis exercise to identify the deficit skills within an organization. The gap analysis shall take into considerations the volatility of the domain and identify factors such as technology changes, organization's information security strategy within the context of an organization.
3. The analysis shall identify gaps both in terms of required resources and the relevant skill sets to effectively implement the organization's information security.
4. Identify the team that needs to be trained, care should be taken to ensure that the relevant skills are spread across the team and there is no concentration or potential single point of failures.
5. Identify and evaluate the training delivery platforms available to the organization. These include online trainings, classroom trainings, self-learning etc. Factors that may impact include time for training, logistics involved, cost of the training, impact on operations etc.
6. A formal assessment process to evaluate the effectiveness of trainings imparted.
7. It would be better to take a long-term perspective and effectively train resources on specific skills track in view of the volatile changes in the domain and the organization's long-term strategy.
8. Employees should be motivated / incentivized for demonstrating their efforts to keep their skillsets current.

7.2.3. Defining and Implementing Processes

Having established the necessary governance in place, a key step is to establish the right processes in place to implement an effective program.

The section below highlights some of the key processes that needs to be in place. Organizations are advised to review the National Information Assurance Policy V2.0 and any regulations issued by the local or international regulators and any other sector specific best practices such as the one issued by IATA.

7.2.4. Information Asset Classification and Labelling

1. The cyber security leadership within the organization should manage the program to classify and label the assets, however it is the responsibility of the information asset owner / business to actually classify the asset.
2. Create an inventory of all information assets across the business along with identifying their owner.
3. Evaluate the aggregate Security Value of the Information asset using an Information Asset Classification Model[6]

[6] National Information Assurance Policy also proposes an Information Asset Classification Model.

4. Evaluate the Data Privacy Impact Assessment to ascertain if the Information asset has any Personal Identifiable Information (PII).
5. Label the information asset based on the Confidentiality and Privacy ratings of the asset.
6. The labels should be clear, unambiguous and visible.
7. For electronic data, it is also recommended to use meta tags or machine readable formats.

7.2.5. Configuration Management

1. Define and implement a Configuration Management process within the organization.
2. Ensure all configurable (active) items within your Information Asset register are clearly identified.
3. Maintain a repository of the most updated and current versions (working) of these information assets including baselines, constituent components, their attributes and relationships.
4. The repository should be secured to maintain its confidentiality, integrity and availability.
5. Work with Change Management to ensure that only authorized components are used, and only authorized changes are made to the information assets.

7.2.6. Change Management

1. Define and implement a Change Management process in line with the NIA Policy[7].
2. Establish a Change Management Board (CMB) or Change Advisory Board (CAB) to review and approve any changes to the system.
3. The CMB / CAB should draw its members from the business verticals, IT Department, Information Security Head, Business Continuity Head and any other members as may be required.
4. The CMB / CAB should approve all the changes.
5. Define an Emergency approval process to carry out any emergency changes, if any are required. This may involve verbal approvals, direct approval from a senior management etc.
6. Notwithstanding, all changes (including emergency changes) should be documented in the change management system.
7. Any change requests should include a rollback process in case if the proposed change is not successful.
8. The process should include regular reviews to ensure that the executed changes have achieved their objectives and are performing well, as well as rolling back changes that were temporary in nature.

7.2.7. System Acceptance and Commissioning

1. Define a process to validate any new system (software / hardware) introduced into the business network.
2. The validation process on a minimum should include:

[7] Templates for Change Management Process maps. Change management forms are available on Q-CERT website.

   a. The business justification and the need for the information asset within the business network.
   b. The information asset classification and labeling of the information asset.
   c. A minimum baseline security assessment that includes:
      i. A check to confirm that standard security controls such as end-point protection, hardening etc. have been implemented.
      ii. A vulnerability assessment exercise to identify any known vulnerabilities.
      iii. An execution plan to either eliminate or mitigate the identified vulnerabilities in line with the risk appetite of the organization.
3. Update the Asset Inventory list after the system has been commissioned.
4. Update the System monitoring solution to collect and monitor security event from the commissioned device.

7.2.8. Logging and Monitoring

1. Define and implement a Logging and Monitoring process in line with the NIA Policy[8].
2. Configure all information assets to log critical system and security logs. Organizations should ensure that adequate events are logged necessary to identify and assist in investigation of security incidents.[9]
3. Protect the logs from tampering.
4. Maintain logs for a minimum of 120 day in line with Cyber Crime Law.
5. Monitor the security logs on a 24x7 basis, at least for the critical systems.
6. It is recommended to correlate logs from various systems be co-related to get a holistic view of the operations.
7. The Logging and Monitoring process should work closely with the Incident Management process and the logging and monitoring system should be able to route incidents identified through the system for incident response.

7.2.9. Incident Reporting and Management

1. Define and implement an incident management process in line with the NIA Policy.
2. Establish mechanisms for users and employees to report information security incidents in a responsible manner.
3. Define a SLA (internal and external) for responding and closing all reported incidents.
4. The information security program should require reporting of all cyber security attacks / incidents targeted on aircraft systems, maintenance and ground support systems for aircraft, airport information systems to Q-CERT and Civil Aviation Authority.
5. Report any cyber-attacks / incidents categorized as Level 1 or Level 2[10], ASAP or within two days of its discovery.

7.2.10. Data Breach Notification

1. Regulations especially in the realm of privacy make it mandatory to inform the data subjects in case of a breach of their personal information with the organization.
2. Define a procedure to notify data subjects upon discovery of a data breach incident.

[8] NIA Policy provides controls to enable Logging and Monitoring.

[9] "Guidelines for Incident Management – Pre-requisite Measures also provides additional system specific guidance.

[10] Refer to Appendix C (Incident Management Criticality Classification" NIA Policy V2.0

3. The procedure should ensure that:
    a. The process integrates with the corporate Incident Management / Crisis Management processes.
    b. Regulations may dictate the period upon breach discovery, within which to carry out such a notification.
    c. The organization has an inventory of data subjects whose personal information exists within the organizations business data.
    d. The organization identifies appropriate communication mediums and tools for notification to data subjects in case of an identified data breach incident.

7.2.11. Business Continuity and Resilience

1. Aviation is a critical sector for Qatar and organizations should ensure that the business is designed to be resilient in the face of natural / man-made calamities, technological disasters and / or accidents.
2. Assign a person to own and manage the Business Continuity program and the associated Business Continuity Management System.
3. Conduct a Business Impact Analysis to identify critical processes and systems and identify their Recovery Time Objective (RTOs) and Recovery Process Objectives (RPOs).
4. While conducting a Business Impact Analysis, the management should also consider events that have the potential to blow out in to a Black Swan[11]
5. Develop a comprehensive Business Continuity Plan (BCP)[12] covering all the critical systems.
6. The BCP should adequately cover the People (Most Important), Processes and Technology.
7. Design critical systems to be fault tolerant and resilient in line with the RTO and RPO requirements.
8. Test the BCP at regular intervals including live tests and failovers to ensure that the BCP will work in case of a disaster.

[11] Black Swan events are those that have a very low probability to occur, but if they do, the impacts are very high.

[12] Refer to National Information Assurance Policy V2.0 and Industry Standards such as ISO 22301 for additional guidance.

7.3. Monitoring the Processes

A successful ISMS program hinges not on the successful creation of processes but its effective usage in the day-to-day operations of the business. It is important that the organizations monitor the processes regularly and take corrective action on an immediate basis to ensure that the process is effective and achieves the defined objectives.

7.3.1. Defining Key Metrics or Success Factors

1. While designing your internal processes, identify the key objectives that you would like to achieve and translate them in to SMART[13] metrics
2. The metrics should be relevant to the process and your business objectives

7.4. Monitoring the Key Metrics / Success Factors

1. Define a mechanism to monitor the assigned metrics for the processes.
2. Monitor the process at regular intervals e.g. Monthly, Quarterly etc.
3. Initially the frequency for monitoring should be high up until such time where you believe that the process has matured and has been fine-tuned.
4. Take immediate corrective action if you observe any anomalies within the process.

[13] SMART: Specific Measurable Assignable Realistic Time Related

8. Technical Controls

The section below highlights some of the key technical controls that needs to be in place. Organizations are advised to review the National Information Assurance Policy V2.0 and any regulations issued by the local or international regulators and any other sector specific best practices such as the one issued by IATA.

A key consideration to me made is to ensure that the chosen controls are wholesome. In a way, the controls should cover all aspects of your business and should be evenly balanced and spread out. Along with the controls that are deterrent, avoiding and preventive in nature, the organizations should also implement controls that can help in detecting, responding and recovering from incidents.

8.1. Section A: General IT Controls

8.1.1. System and Network Design

Organizations should ensure that security is imbibed in the architecture (Systems and Networks) by design rather than add-ons put in to mitigate design flaws. On a minimum, consider the following factors:

1. Segmentation: Segregate information assets in different segments (security zones) based on their criticality or aggregate security level (as derived from the information classification exercise).
2. Access Surface: Access to information assets should be restricted to limited and regulated communication channels only. Further, only make available information that is required. Hide all other information as much as possible reinforcing the concept of "Security by Obscurity".
3. Defense in Depth: Protect the Information asset at multiple levels and points using multiple techniques and technology. The security of the system should be assessed against the least secured asset in the system (weakest link).
4. Adequate Protection: The security controls chosen should be adequate and appropriate based on the Risk profile of the organization and the risk to the asset itself as well as the value of the asset itself.
5. Least Privilege / Need to Know: Access to the information assets should be carefully controlled and restricted based on the concepts of least privilege or a Need to Know basis. Special attention should be placed on Administrative or Privileged accounts.
6. Privacy By Design: Protection of Personal Information is a key regulatory requirement both locally as well as internationally. The regulation enshrines a number of rights to the individuals such as Right to be forgotten, Right to information, Need for consent etc. It is necessary that the systems be designed in line with the privacy regulatory requirements.
7. Availability: Design systems based on their availability requirements. For systems that need high availability, Protect them against single point of failures, using redundant elements and high availability concepts.

8.1.2. System and Network Security

The NIA Policy covers in depth controls for system and network security. The section below reprises the most important ones:

1. Configuration:
   a. Secure the configuration of all network and security devices.
   b. A copy of updated and tested configuration should be stored in a secure location to be used in case of a disaster.
2. Diodes / Firewalls / Proxy:
   a. Segregate the most critical systems using Diodes. Diodes are unidirectional.
   b. Use Firewalls to compartmentalize the systems as per different security zones.
   c. Use an appropriate firewall to regulate traffic (application / packets / protocols / ports) based on the OSI Network model.
   d. Configure the firewall with appropriate and granular rules.
   e. Route any traffic from internet through a proxy server.
3. Clock Synchronization:
   a. Configure a Network Time Server to synchronize all devices on the network to the same time source.
4. Wireless Security
   a. Maintain an inventory of Wireless Access Points. Monitor, detect and remove rogue wireless access points.
   b. Configure the system to use adequate authentication and encryption.
   c. Use firewall / routers to segregate the networks. Use different SSIDs and different configurations for networks of varying security zones.
   d. Adequate security measure should be followed when installing your public Wi-Fi, refer to our Cyber Security Guidelines for Public Wi-Fi[14]
   e. Also, refer to our Cyber Security Guidelines for Securing Home and Small Office Routers[15] for your routers and access points setup recommendations.
5. DNS
   a. Use separate Domain Name Servers for resolving internal and external addresses.
   b. Zones files are digitally signed, and cryptographic mutual authentication and data integrity of zone transfers and dynamic updates is provided. Cryptographic origin authentication and integrity assurance of DNS data is provided.
6. VPN
   a. Any remote connections to the business systems should be through a VPN.
   b. Connections to business critical systems should be through a VPN, even when connecting through business wireless systems.
   c. Treat the traffic from a VPN connection in the same way as business traffic and filter them through the same checks (monitoring and control).

[14] http://www.qcert.org/sites/default/files/public/documents/cs-csps_guidelines_for_public_wifi_eng_v1.0.pdf

[15] http://www.qcert.org/sites/default/files/public/documents/cs-csps_guidelines_home_office_routers_en_v1.0.pdf

7. System Hardening
    a. All systems should conform to a minimum baseline posture. On a minimum these should include:
        i. Application of all known security patches.
        ii. Disable all unwanted services and uninstall all unwanted applications.
        iii. Enable necessary logs for audit and system and security monitoring[16].
        iv. Install endpoint protection program e.g. Anti-Malicious software, HIDS, Application Firewall etc.
        v. A Vulnerability assessment (esp. for servers) to identify known vulnerabilities.
    b. The organization should define Hardening Profiles for the various systems it uses based on the security requirements.
    c. Ensure protection against DDOS attacks. The Cyber Security Guidelines for Distributed Denial of Service[17] (DDoS) Attacks provides guidance and recommendations for the same.
8. Endpoint Security
    a. Register each endpoint in the Information Asset register.
    b. Install a tested Anti-Malicious program on all systems.
    c. Log, monitor and address alerts from the endpoint security system.
    d. Configure Host based Intrusion Detection Systems (HIDS) and / or Application Firewalls on servers.
    e. Evaluate and install Data Leakage Protection solutions for endpoints that have access to business critical data and / or PII data of your customers / employees.
9. Privacy By Design
    a. For every new information asset introduced into the system:
        i. Update the Information Asset Register.
        ii. Identify the PII that it creates, processes or stores.
        iii. Conduct a Data Privacy Impact Assessment (DPIA) to identify the criticality of the data and the potential security controls to secure the PII.

8.1.3. Communication Security

The NIA Policy covers in depth controls for communication security. The section below reprises the most important ones:

1. Encrypt all communications (to the extent possible).
2. Besides the NIA Policy, MOTC (PKI Section) has also issued standards for encryption algorithms[18].
3. Communication Equipment:
    a. Physically protect the cables and the communication equipment against tampering, sabotage or accidental damage.

[16] Refer to Guidelines to Incident Management – Pre-requisite Measures

[17] http://www.qcert.org/sites/default/files/public/documents/cs-csps_cs_guidelines_ddos_attacks__eng_v1.0.pdf

[18] http://www.qcert.org/sites/default/files/public/documents/electronic_signature_overview___specification_v1.0.pdf
http://www.qcert.org/sites/default/files/public/documents/electronic_signature_algorithms_standard.pdf

   b. Use recommended protocols and algorithms that are as secure as possible.
   c. Evaluate the security of the protocols and algorithms used and implement compensating controls to ensure the confidentiality, integrity and availability of the signals.

8.1.4. Product Security

The NIA Policy covers in depth controls for product security. The section below reprises the most important ones:

1. Any product chosen to solve a business problem or meet a business requirement should:
   a. Be supported by a vendor of good standing and commitment.
   b. Be selected through an independent and unbiased process of vendor / product selection.
   c. Be independently tested to ensure that it meets all the business and security requirements of the business.
2. A minimum-security assurance levels is assured for products chosen for critical business functions including those used in airplanes e.g. Common Criteria. In addition, equipment used in airplanes should be part of the Air Worthiness check in an airplane.
3. Ensure that the products do not contain any hardcoded usernames and passwords. All default passwords should be changed prior use in business networks.

8.1.5. Software Security

The NIA Policy covers in depth controls for software security. The section below reprises the most important ones:

1. Adhere to and imbibe security controls within the software development cycle (SDLC).
2. Secure SDLC include BSIMM and OSAMM methodology amongst others.
3. Test the security of any software deployed in business networks. Testing includes Vulnerability Testing, Penetration Testing, Code Reviews etc. Perform code reviews for the most critical applications.
4. Review and adhere to the guidelines provided by MOTC[19], if the organization intends to use Open Source Software.

8.1.6. Cloud Security

The Cloud Security Policy[20] covers in depth controls for software security. Further, the Data Location advisory[21] provides additional guidance on using CSPs located outside Qatar.

1. Organizations should host critical business data inside Qatar (to the extent possible) or in countries that have friendly (political) relations with and regulatory regimes similar to Qatar.

[19] http://www.qcert.org/sites/default/files/public/documents/cs_guidelines_open_source_software_eng_v1.0_0.pdf

[20] http://www.qcert.org/sites/default/files/public/documents/cs_cloud_security_policy-2017_english_v1.2.pdf

[21] http://www.qcert.org/alerts/data-location-advisory-v20

2. Encrypt data stored outside Qatar for regulatory or business continuity requirements.
3. Personal data (PII) stored / processed in clouds should meet the Data Privacy regulatory requirements both locally as well as internationally.

8.1.7. ICS / IoT Security

The Smart Qatar Security Standard[22] covers in depth controls for IoT security.

The ICS Security Standard[23] covers in depth controls for ICS security

8.1.8. Identity and Access Management / Privilege Access Management

The Qatar e-Authentication Framework[24] provides a strong framework for building an e-Authentication solution within an organization.

The NIA Policy covers in depth security controls for Identity and Authentication Management.

8.1.9. Cryptography

The NIA Policy covers in depth security controls for Cryptography. Besides the Certificate Service Provider – Management Authority within MOTC has also issued standards and guidance related to use of Cryptography. The section below reprises the most important ones:

1. Use encrypted communication wherever possible especially within critical business units and systems.
2. Ensure the algorithm used is appropriate and of adequate strength. The NIA Policy as well as the standards issued by the CSP-MA in MOTC, recommend the most appropriate technologies and algorithms to be used.
3. Cryptography is as much about the processes as it is about the technology. Make sure you have adequate processes in place to ensure the integrity and confidentiality of certificates issued throughout its life cycle.

8.1.10. Media Security

The NIA Policy covers in depth security controls for Media Security. The section below reprises the most important ones:

1. Security controls for media should consider privacy impacts along with security considerations.
2. By design, do not retain data / media beyond what is required. For as long as data / media is retained (throughout its life cycle and in all forms), it should be protected as per its security profile.
3. Practical and adequate data disposal means should be implemented to dispose data that has served its purpose and needs to be destroyed.

[22] The Smart Qatar Security Standard can be made available on request.
[23] http://www.qcert.org/sites/default/files/public/documents/national_ics_security_standard_v.3_-_final.pdf
[24] http://www.qcert.org/sites/default/files/public/documents/cs-gima-qatar_e-authentication_framework_v1.0_0.pdf

8.1.11. BYOD

The BYOD Security Policy[25] covers in depth security controls for any personal device used in the business network / system. This includes any devices such as storage (USBs), wireless routers, mobiles / tablets etc. In addition, the NIA Policy also includes controls for BYODs.

8.2. Section B: Airport Information Systems

8.2.1. General Controls:

1. Critical system and its core components should be evaluated for CC / EAL certifications on a minimum level 3 / 4
2. Technical Security evaluations of systems. These includes Vulnerability assessments (Penetration Testing), Compliance Reviews, Network Traffic Review, and System Configuration Reviews, Network discovery, port and protocol identification.

8.2.2. System Specific Controls

8.2.2.1. Baggage Handling Systems

1. Implement the controls within the ICS Security standards to secure the Baggage Handling Systems.
2. Segregate all critical systems such as the baggage handling systems in to separate networks on the system. Such segregation could be either physical or using firewalls or diodes.

8.2.2.2. Departure Control Systems (DCS)

1. Encrypt all information within the system.
2. Create awareness for users on the potential PII that is available on documents such as copies of tickets, visas, boarding passes etc.
3. Any information on paper media should be disposed securely.

8.3. Section C: Air Navigation Systems (Air Traffic Control Systems)

8.3.1. General Controls:

1. Critical system and its core components should be evaluated for CC / EAL certifications on a minimum level 3 / 4
2. Protect Data and Information are prime assets, as well as the associated networks and systems handling these data and information. These include:
   a. Flight operational and planning data: examples include aircraft trajectory, RNP data, and ACARS messages on air-ground communications
   b. Weather and traffic surveillance data: examples include ADS-B-In, FIS-B, TIS-B, aircraft weather sensor data shared on air-ground and air-air communications
   c. Position, navigation and timing data: examples include GNSS, ADS-B-Out
   d. Aeronautical information services and meteorological data: examples include real-time updates on meteorological conditions and airport conditions; emergencies and restrictions that limit airspace use during flight

[25] http://www.qcert.org/sites/default/files/public/documents/cs-csps_byod_policy_v1.0.pdf

e. Controller-pilot automated messages and voice communications: examples include the two-way communications that replace voice communications with data link of automated messages and receipts
f. Aircraft status data: examples include cabin and flight deck videos
g. Airport surface area communications: examples include airport surface area operations data
h. Security relevant data: examples include digital certificates, keys, credentials, and passwords

3. Where possible ensure that aviation communication between the aircrafts and the ground ATC systems is authenticated and encrypted to protect against threats such as Eavesdropping, Jamming and Message Injection, Message Deletion and Message Modification.
4. Design systems for high availability and redundancy.
5. Use IPV6 where possible as this version of TCP/IP has IPSec encryption by default.
6. Networks used in aircrafts should not share the same frequencies / or the bus as those used by the avionics.
7. In case the VHF, UHF and HF ATC tower voice systems are integrated; through a LAN (TCP/IP) network, ensure that measures are taken to mitigate against SNMP and Voice over IP (VOIP) vulnerabilities.
8. Technology to jam Wi-Fi and radio frequencies around the airports for targeted areas should be implemented to block unauthorized UAVs approaching the perimeter for both Wi-Fi (2.4 GHz and 5 GHz bands) as well as radio signals. This would result in the remote control (ground unit) to lose signal to communicate to UAV immediately, forcing the UAV to either return home or land based on its configuration.
9. Investigate use of Cryptography scheme for ensuring the integrity and imitation protection of air navigation infrastructure from cyber attacks.

8.3.2. System Specific Controls

8.3.2.1. Large-scale Information Sharing Infrastructure

This includes information sharing between multiple users and applications for worldwide collaboration for aviation tasks. Examples include - aeronautical-specific infrastructure such as SWIM, ISDN - public infrastructures such as cloud computing and Internet.

1. Validate the information input process to ensure that it is consistent with the expected content? (e.g. validation against protocol specifications, message definitions).
2. Protect the data integrity and origin authentication using cryptographic methods.
3. Use encryption to protect the confidentiality of sensitive information exchanges.
4. Uniquely identify users, services and devices in the ICT support systems.

8.3.2.2. Air Navigation Support Infrastructure

This includes infrastructure deployed extensively for air-ground communications and passive/active monitoring and tracking of aircraft positions. - ground-based transponders for air-ground communications - positioning systems (e.g., GBAS, multilateration stations) and radars for supporting air traffic control - satellites as communication relay and navigation support infrastructure - airport surface area network (e.g., ASDE, WiMAX based AeroMACS).

1. Validate the information input process to ensure that it is consistent with the expected content? (e.g. validation against protocol specifications, message definitions).
2. Protect the data integrity and origin authentication using cryptographic methods.
3. Use encryption to protect the confidentiality of sensitive information exchanges.
4. Uniquely identify users, services and devices in the ICT support systems.

8.3.2.3. Electronic flight bags (EFBs)

Electronic Flight Bags act as electronic replacements for paper documents carried by pilots. It can include aeronautical charts, approach plates, aircraft manuals, and checklists. In its simplest form, it is not much more than PDF viewers for these documents, but more sophisticated versions that provide features such as interactive checklists. The use of EFBs in air carriers requires FAA approval and regulations that prohibit the use of certain functionality such as "own-ship position" in this environment. These limitations do, however, not exist for general aviation.

EFBs come in three classes.
Class 1 is the most simple of the three and simply involves electronic documents that store and display on e-readers like the Amazon Kindle or the iPad. These devices normally are stowed during takeoff and landing, and do not require an administrative process to remove them from the aircraft. Class 1 EFBs are not connected directly to aircraft systems.
Class 2 EFBs are something different. These devices are based on tablet computers like the iPad, but have mounting brackets and docking stations that connect them directly to aircraft systems while the aircraft are in flight or operating at airports.
While Class 2 EFBs offer the convenience of enabling the pilot to take them quickly out of the aircraft for use on the ground, they also have secure and encrypted wired or wireless connections to the aircraft systems to enable pilots to send and receive reports and forecasts during flight, and interface with aircraft navigation systems to display moving maps.
Class 3 EFBs, meanwhile, are permanent fixtures in the cockpit like other avionics instruments. They are hard-wired with secure links into aircraft navigation systems and flight computers, and offer expanded capabilities like automatic dependent surveillance-broadcast (ADS-B) cooperative surveillance.
Class 3 EFBs only can be removed from the aircraft by certified maintenance personnel, and each removal and installation must be documented in maintenance logs.

1. EFBs exist in a segregated secure zone and access to any other information systems on the airplane or with the ATC or ground systems is controlled through a granularly configured firewall.
2. The device (EFBs) is hardened for specific use and only specific whitelisted applications are installed on it.
3. Portable (COTS) devices that are used as EFBs should implement controls specified in the BYOD Security Policy.

8.4. Section D: Aircraft Systems

8.4.1. General Controls:

1. Critical system and its core components should be evaluated for CC / EAL certifications on a minimum level 3 / 4

2. Incorporate cyber security assessment requirements for air carrier operating certificates and production certificates.
3. IMA systems should be separated from other systems preferably physically using firewalls and Diodes.
4. Where IMA applications are co-hosted with less critical applications, it should conform to ARINC 653 [26]standards

8.4.1.1. System Specific Controls

8.4.1.2. Avionics

Integrated Modular Avionics

1. Wireless Maintenance Log Systems.
    a. Perform a detailed Risk Assessment as per Industry best practices.
    b. Wherever possible, implement encryption and encoding for end-to-end communications.
    c. Segregate the maintenance and corporate networks.
2. Fly By Wireless Systems / Wireless Avionics Systems
    a. Perform a detailed Risk Assessment as per Industry best practices.
    b. Wherever possible, implement encryption and encoding for end-to-end communications.
    c. Segregate the maintenance and corporate networks.
    d. As a Safety Plug, some type of pilot intervention should be available to mitigate the risks of a failure of an auto-pilot.
    e. Implement a software assurance program for the critical applications including auto-pilot.
3. Push towards Cloud based systems by operators
    a. Evaluate cloud service against the Cloud Security Policy issued by MOTC.
    b. Implement two factor authentication between the client and cloud services.
4. The IMA should comply with standards such as ARINC 653 specifications

8.4.1.3. In-flight Entertainment (IFE) Systems

1. Do not use hard coded usernames or passwords in the IFE systems.
2. Regularly scan and patch vulnerabilities in the IFE systems.
3. The IFE system should be physical segregated from the other airplane systems. If this is not feasible, organizations should use Diodes as a mitigating control to prevent data flow from IFE systems to other airplane systems.

8.5. Section E: Airline Systems

8.5.1. Ticket Booking Portal

The security controls mentioned in the Software security and the Product security section above, along with the NIA Policy are applicable for the e-commerce (Ticket Booking) portal as well. Pay special attention to the following aspects:

[26] American Standard ARINC 653: Industrial Standard for integrity of safety critical IMA application.

1. Authentication: Using digital certificates from trusted authorities (preferably Qatari CSPs[27]) to validate the identity of portal service provider.
2. Privacy:
   a. Only collect data that is required. Dispose of data once the requirement is complete (including regulatory requirements).
   b. Encrypt data throughout its life cycle from collection, processing, storage and disposal.
3. Integrity: Integrity of information means ensuring that a communication received has not been altered or tampered with. In an e-commerce portal, this can be achieved by using digital certificates to digitally "sign" messages.
4. Segmentation: Ensure proper segmentation between web servers and database servers. Utilize a DMZ for internet facing assets to prevent an attacker from gaining direct access to internal assets in the event of a breach.
5. Availability: Define a back-up strategy for databases and applications. Consider off-site storage for critical data.
6. Non-repudiation: Non-repudiation is the ability, to legally prove that a person has sent a specific email, requested a service, or made a purchase approval from a website. In the realm of e-commerce, nonrepudiation is achieved by using digital signatures.
7. PCI Compliance: Ensure that your payment gateway is in compliance to PCI standards. The organizations should take extra care in selecting their POS system vendors and credit card processors. The third party agreements with these entities should be vetted and security obligations should become part of such agreements
8. Testing: Regular testing of the e-commerce portal to:
   a. Verify the security requirement specification such as location of the asset(s), access control mechanism for the assets, operational context of the organization, existing system services and their access control mechanisms, and the connectivity within the organization and connectivity of the organization to the outside world
   b. Verify the configuration of the security tools specified in the security infrastructure i.e. whether the security tools are properly installed and configured to maintain the security of the asset
   c. Verify that all known patches are updated or suitably mitigated.
   d. Verify if any gap exists between the proposed security infrastructure and the implemented security infrastructure
   e. Verify the limitation of the proposed security infrastructure with respect to the known vulnerabilities

8.6. Section F: Physical Security

Physical Security is an important element within a cyber security strategy for an organization. It is essential that information in its physical form (papers, digital media, computing machines) is protected as much as its virtual form. A physical breach can endanger and potentially bypass most of the logical controls that may be in place to secure the information asset.

[27] CSP here means Digital Certificate Service Provider

Agencies should ensure that the physical security procedures for their organizations should include on a minimum:

1. Detailed Risk assessment of the site, assessing each site against the activity that it carries out, the threats, vulnerabilities and overall risk to the organization.
2. Based on the above adequate controls should be defined and implemented.
3. The effectiveness of these controls should be assessed on a regular basis and extraordinarily in case such a control has been breached. The exercise will recommend corrective measures to ensure that the controls continue to provide the expected level of operations.
4. A detailed documentation will be maintained which will include documents such as Civil drawings of the site, floor plans, electrical and wiring diagrams, emergency plans and exits.
5. The physical security procedures shall give utmost importance to the safety of the humans working at the site.
    a. Employees, contractors and visitors to the site should be briefed on basic security measures.
6. Strictly control the physical access to computer systems or avionics or communication systems abroad an aircraft. Where possible and for critical systems, a principle of four eyes should be used.
7. Carry out regular tests on the security access controls system.
8. The controls chosen by the organization should on a minimum comply with:
    a. Guidelines and recommendations from ICAO
    b. Local Civil Defense requirements
    c. NIA Policy Section C – 12 Physical Security along with controls provided in Appendix A.

9. Cyber Insurance

A data security breach is an incident in which the confidentiality, integrity or availability of data (often stored electronically) is compromised, such that the data is vulnerable to access or acquisition by unauthorized persons. Not all data breaches are caused purposefully by hackers or malevolent individuals; some are caused by individual carelessness, such as leaving an unsecured laptop somewhere and exposing the data to an unsecured environment. With personally identifiable information — such as QID numbers, financial account numbers or access credentials — the loss of confidentiality potentially can lead to identity theft, unauthorized credit or debit card charges, and bank account fraud. Airlines could experience direct and indirect losses, including fines and penalties imposed by the card associations. Companies may also face third-party liability in the form of lawsuits and claims, regulatory fines, and, in some cases, even civil and criminal penalties.

Cyber Insurance is not a line of defense, however in case of an event such as Black Swan or a breach, it can help organizations manage some of the liabilities at least from a financial perspective. This makes sense in a strong regulatory environment where organizations may be liable of disciplinary fines and / or costs related to breach notification.

Agencies should be careful and due diligence should be conducted, including involving business stakeholders such as Legal department while negotiating an appropriate Cyber insurance policy for the agency. All definitions and its interpretations by both the policy owner and the cyber insurance provider should be vetted by the legal department. Some of the factors to consider while choosing a cyber insurance cover are:

Type of Cover: Typically the policy should cover both first-party and third-party losses suffered as a result of a cybersecurity breach.

Scope of Coverage: The scope of coverage can be tailored to a variety of risk scenarios and should cover the following:

- **Asset Liability** covers digital assets replacement expense coverage, business incomes loss and dependent business income loss coverage, cyber extortion threat and reward payments coverage.
- **Network Security Liability** covers third-party damages resulting from a failure to protect against destruction, deletion, or corruption of a third party's electronic data. This could be the result of a denial of service attacks against websites or computers, or through the transmission of a virus from third-party computers and systems.
- **Privacy Liability** covers third-party damages that result from the disclosure of confidential information collected or handled by you, or that is under your custody or control. This includes coverage for vicarious liability where a vendor loses information you had entrusted to them.
- **Electronic Media Content Liability** covers personal injury, and trademark/copyright claims that arise from the creation and dissemination of electronic content.
- **Regulatory Defense and Penalties** covers costs arising from an alleged violation of privacy law caused by a security breach.
- **Network Extortion** provides reimbursement for payments made under duress in response to an extortion threat.

- **Network Business Interruption** provides reimbursement for your loss of income and extra expenses that result from an interruption or suspension of computer systems. This includes limits placed - dependent business interruption losses.
- **Breach Event Expenses** covers costs associated with privacy regulation compliance. This includes retaining a crisis management firm, outside counsel, legal costs, regulatory fines, breach notification or forensic investigators.
- **Data Asset Protection** covers recovery of costs and expenses that you may incur to restore, recreate, or recollect your data and other intangible assets.
- **Multimedia/Media liability** covers can include specific defacement of website and intellectual property rights infringement.
- **Extortion liability** covers losses due to a threat of extortion, professional fees related to dealing with the extortion.
- **Third-party claims**. This includes claims for damages brought by customers, consumers or outside business entities for damages they incurred as a result of the insured company's breach of security, namely their losses from the inability to transact business, including punitive and exemplary damages, settlements and costs.

The above lists are not exhaustive, Carriers may offer additional coverage, especially for companies with specialized risks.

Time Limit: is defined as the duration for remediation coverage, the most common time period is one year after the breach.

Geographic spread of operations: Companies with a global footprint face different risks in different jurisdictions. The US for example is a fairly litigious environment with significant privacy laws and regulations, creating significant exposure. Other jurisdictions may not have robust regulation or enforcement, reducing the risk of exposure from a breach.

Exclusions: Cyber policies often contain a host of exclusions. Agreement on the wording of many of these exclusions — and therefore their scope — are an important part of the negotiation process. Possible exclusions from cyber policies should be carefully noted and, if feasible, negotiated around.

Examples of some exclusions include:

- **Contractual liability exclusion.** This exclusion typically functions to exclude coverage for any liability assumed by an insured under a contract or agreement.

- **Criminal conduct exclusion.** Many policies contain exclusions for criminal or fraudulent acts by the insured.

- **Exclusion for terrorism, hostilities, and claims arising from "acts of foreign enemies".** This exclusion could bar coverage where a cyber attack or breach originates in a foreign country and arguably occurred at the direction of a hostile foreign government.

- **Exclusion for unauthorized collection of customer data.** Some policies contain exclusions for losses related to data whose collection was not authorized.

Limitations: Cyber Policies may include limitations introduced either by the insured or the provider. The agency needs to understand the impact it will have on its coverage. E.g. Geographical limits requested by the insured may impact premiums but may impact notifications costs. Many policies limit coverage for notifications to a set number of persons. Certain providers may impose limitations on the choice forensics investigators

Appendix I provided at the end of the document provides a list of additional questions that may assist the agencies in choosing the right Cyber Insurance Policy / cover for their organization.

10. Supply Chain Security Management

Supply chain security is a program that focuses on the potential risks associated with an organization's suppliers of goods and services, many of which may have extensive access to resources and assets within the enterprise environment or to an organization's customer environments, some of which may be sensitive in nature.

10.1. Vendor Management Program

A key to an efficient Supply Chain security management program is to have a formal Vendor Management Program in place. The program should identify the primary / secondary contacts for each vendor. Although it might help to have a single point of contact, certain business / volume may merit having subject matter point of contacts.

An agency should establish a vendor management policy to establish guidelines and controls to ensure consistent processes and sufficient oversight to manage the monitoring of key vendors and outsourced service providers. The policy should define:

1. An owner for managing the vendor management program.
2. A procedure to classify the vendors that provide service to the organization.
3. A procedure to conduct due diligence on vendors that may include on-site and/or remote audits, review of vendor policies and procedures.
4. Training for all responsible parties
5. Monitoring vendor performance / SLAs / compliance etc
6. Regular reporting to senior leadership using a risk based approach, relying on judgment and expertise as well as standard processes and categorization.

10.2. Vendor Classification

An airplane manufacture is a classic case study of Supply Chain Management. An organization designs and assembles the plane whereas a host of other companies possibly from across the globe may manufacture the sub-assemblies and the sub-parts.

Not all parts are critical in the plane assembly and operation and so are the associated vendors providing them. Agencies should have formal procedures in place to identify their vendors, the services / support / equipment they provide and the criticality of the services to which they cater to. Based on these factors the agencies should be able to define the criticality of the vendors.

Criticality Level	Description
CR3	The vendor is very Critical. The services he caters to are critical to the functioning of organization and / or the key services delivered by organization. There are no / very few competitors providing the same service
CR2	The vendor is Critical. The services he caters to are critical to the functioning of organization and / or the key services delivered by organization. There are sufficient competitors providing the same service.
CR1	The vendor is Important. The services he caters to are important to the functioning of organization and / or the

	services delivered by the organization. There are sufficient competitors providing the same service.
CR0	The vendor is not critical. The services he caters to are not critical to the functioning of the organization.

10.3. Oversight on Vendors

The vendor management program should define a framework with adequate controls for managing the vendors based on their classification.

The framework should ensure:

1. The right to audit and test the security controls of vendors and service providers annually, upon significant changes to the relationship and in response to audit requests or events.
2. A remediation process should be in place to handle non-compliance in an effective and time bound manner.
3. Vendors to adhere to security monitoring requirements. Periodic reports from the vendors and service providers demonstrating service level attainment and performance management.
4. Vendors and service providers should have incident handling procedures and provide timely notification pursuant to any security breaches or incidents that may cause impact to the organization.
5. Controls based on the criticality of the vendors should be implemented across the people, process and technology verticals.
    a. Background checks on employees outsourced / employed at regular intervals. The interval may be defined on vendor criticality.
    b. Communication on role changes / employee changes within the vendor's team, ensuring rights related to the roles are managed accordingly.
    c. Effective skills training covering information security awareness.
    d. Solutions to prevent Data Leakage and Theft within the organization.
    e. Contracts / RFPs issued should identify necessary standards for compliance and have adequate controls defined to ensure compliance.
    f. Software development should adhere to established secure software development life cycle (NIA Policy Section C6 "Software Security")
    g. For critical systems, a code review should be performed, with the vendor submitting a report on its security assessment.
    h. For mission critical systems, software should comply to a minimum Common Criterion Assurance Level of 4*
    i. Patches developed for system should ensure a similar quality and security assurance process prior application in the live systems.
    j. Agencies / Vendors should define a process for Privilege Management.
    k. Critical products and vendors should commit to security of the products and its services throughout the development and its life cycle.
    l. Any activity that may or have the potential to disrupt the product or associated services shall be immediately notified to the customer. This includes any major disruption to the development site, any potential merger and acquisitions, bankruptcy etc.

Appendix A – Risk Management

This guideline would like to make pointers to the following two documents for the purpose of assisting agencies in conducting risk assessments and managing risks.

1. IT Risk Management Framework – Q-CERT, Ministry of Transport & Communications.[28]
2. IT Risk Framework – IATA Guidelines[29]

[28] http://www.qcert.org/library/36
[29] https://www.iata.org/publications/store/Pages/aviation-cyber-security-toolkit.aspx

Appendix B – Information Disclosure Form

The form should include the following information:

Information provided by the Agency

1. Identification of the system that was targeted
2. Description of the effect on the safety of the aircraft as a result of the cyber attack
3. Root Cause Analysis of the attack / incident.
4. Description of the measures taken to counter or mitigate the cyber attack

Information amended by CAA / Q-CERT

1. Analysis of the threats and vulnerabilities used in the attack / incident
2. Recommendation for preventing future attacks
3. Recommendation for improving the regulatory oversight.

Appendix C - Incident Management

This guideline would like to make pointers to the following two documents published by Cyber Security (Q-CERT) for managing cyber incidents.

1. Incident Handling Handbook V2.1

   CS-IH_Handbook ver 2.1.pdf

2. Guidelines for Incident Management – Prerequisite Measures v1.0

Incident Reporting Template

Incident Identification Information	
Incident Number	
Date of Notification (DD/MM/YYYY)	
Time of Notification (HH-MM-SS)	
Incident Detectors Information	
Full Name	
Title	
Contact Info.	
Date/ Time of Detection	
Location	
System or Application	
Incident Summary	
Incident Category	□ Abusive Content / Defacement □ Malicious Code □ Information Gathering □ Intrusion Attempt □ Intrusion / Unauthorized Access □ Unplanned Downtime/ Availability □ Unauthorized Use / Fraud □ Denial of Service □ Other
Incident Criticality	□ Level 1 – High Impact □ Level 2 – Medium Impact □ Level 3 – Low Impact □ Level 0 – No Impact
Description of Incident	

Names and Contact Info. Of involved Parties	Name: Contact Info: Involvement: Name: Contact Info: Involvement:
Incident Notification	
Internal	□ Executive Management □ Security Leadership □ System or Application Owner □ Security Incident Response Team □ Public Affairs □ Legal Council □ Building Administration □ Human Resources □ Information Technology □ Others
External	□ Q-CERT □ Clients or Customers □ Regulatory Agency □ Public □ Emergency Services □ Service Provider or Vendor □ Others
Actions	
Identification measures (incident verified, assessed, options evaluated)	
Containment Measures	
Evidence Collected (System logs etc.)	
Containment Measures	
Eradication Measures	

Recovery Measures	
Other Mitigation Actions	
Evaluation	
How well did taskforce members respond?	
Were the documents procedure followed? Were they adequate?	
What information was needed sooner?	
Were any steps or actions taken that might have inhibited the recovery?	
What could taskforce members do differently the next time an incident occur?	
What corrective actions can prevent similar incidents in the future?	
What additional resources are needed to detect, analyze and mitigate future incidents?	
Other conclusions or recommendations	
Follow-Up	
Reviewed by	□ Executive Management □ Security Officer □ IT Department □ Privacy Officer □ Legal Council □ Other

Recommended actions carried out
Initial report completed by
Follow-up completed by

Appendix D: List of Threat Agents

Humans	Non Humans
Internal – General Employees Physical Security Staff Janitors / Cleaning Staff IT Staff IT Super Users Management Outsourced Staff	IT Malfunctions - Software Bugs Malicious code Computer Component Failure Equipment breakdown Network Failure Hardware Failure Corruption of configuration Application failure/malfunction
External – Malicious Actors – Script Kiddies Cyber Criminals Criminals (Physical) Hacktivists	Nature - Earthquake Flood Rivers Dikes Dams Rain Lightning Strikes Power Surge Fire Wind Tornadoes Hurricanes
External – State Actors	Physical Environment - Electrical Fire Blackouts Brownouts Unannounced Power- Failure (electrical maintenance) Localized Power Failure (single floor; e.g., electrical maintenance) Spontaneous Combustion Fire Water Sprinklers Washrooms (Water Closets)

	Damaged Plumbing (accidental breakage or freezing) Condensation Air Dust Noxious Fumes Pests Ageing of paper media
	Malicious Code - Trojan Horses Viruses Macro Viruses Application Programs (errors in source code)
	Explosive Devices - Bombs
	Jammers
	Arson - Fire
	False Alarms

Appendix E: Human Threat Rating Table

Threat Agent Capability and Motivation Ratings

Capability	Rating	Motivation
Little or no capability to mount an attack.	**Little**	Little or no motivation. Not inclined
Moderate capability. Has knowledge, skills to mount attack, lacking in some resources. Or lacking some knowledge but has sufficient resources to mount an attack.	**Moderate**	Moderate level of motivation. Would act if prompted, or provoked.
Highly capable. Has knowledge, skills and resources to mount an attack	**High**	Highly motivated. Almost certain to attempt an attack

Threat Rating Combinations

Probability Rating	Consequences Rating		
	1	**2**	**3**
1	**1**	**2**	**3**
2	**2**	**3**	**4**
3	**3**	**4**	**5**

Overall Human Threat Ratings

Rating	Description	Level
1	Little or no capability or motivation.	**Low**
2	Little or no capability, moderate level of motivation. Or, moderate capability, little or no motivation.	
3	Highly capable, little or no motivation. Or, little or no capability, highly motivated. Or, moderate capability, moderate level of motivation.	**Medium**
4	Highly capable, moderate level of motivation. Or, moderate capability, highly motivated.	**High**
5	Highly capable, highly motivated.	

Appendix F: Non Human Threat Rating Table

Threat Agent Capability and Motivation Ratings

Probability	Rating	Consequences
Little or no probability of the threat occurring	**Little**	Little or no consequence
Moderate probability	**Moderate**	Moderate consequences
High probability	**High**	High consequences

Threat Rating Combinations

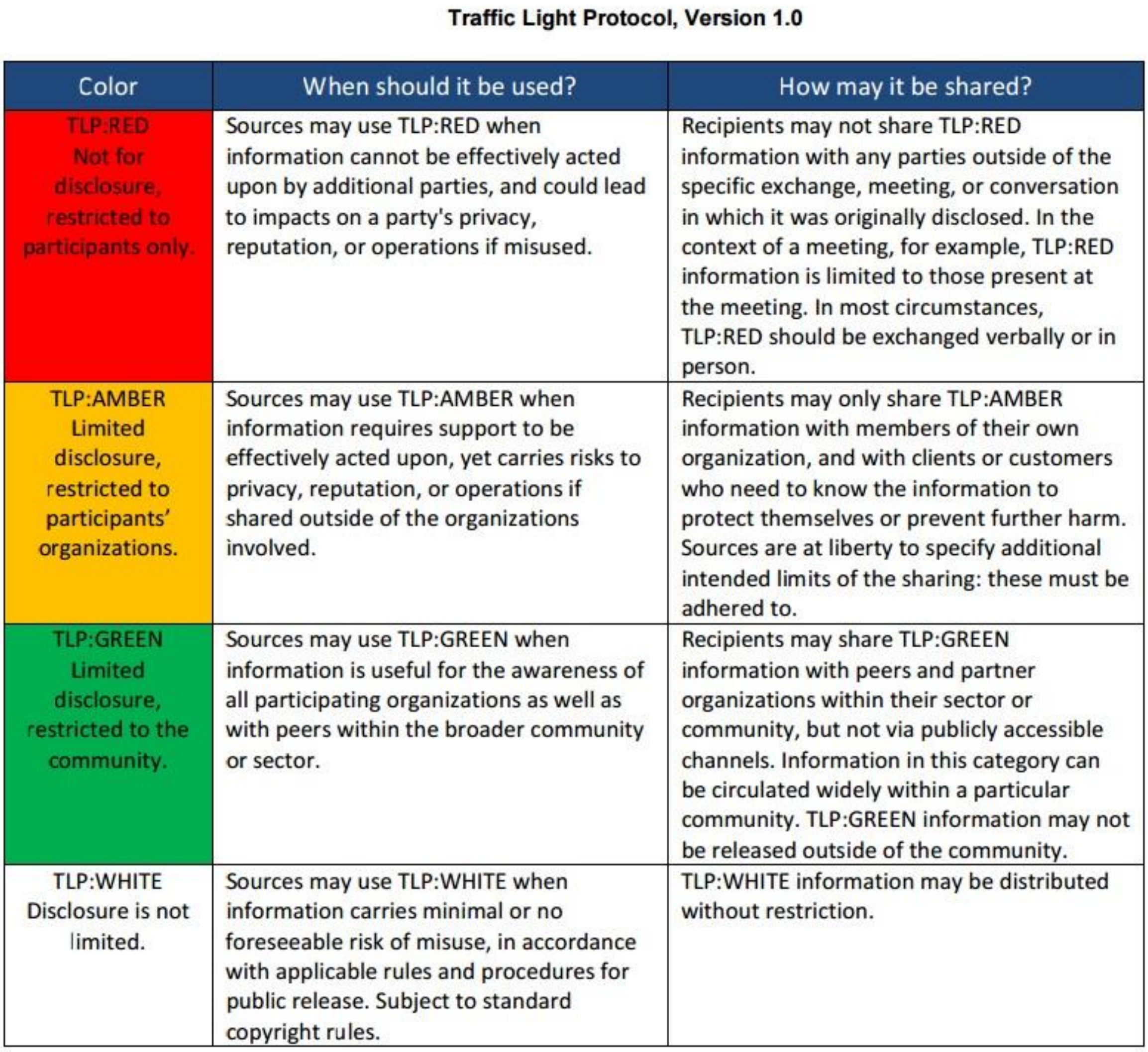
Probability Rating	Consequences Rating		
	1	**2**	**3**
1	**1**	**2**	**3**
2	**2**	**3**	**4**
3	**3**	**4**	**5**

Overall Threat Ratings

Rating	Description	Level
1	Little or no probability or consequences	**Low**
2	Little or no probability, moderate consequences. Or, moderate probability, little or no consequences.	
3	High probability, little or no consequences. Or, little or no probability, high consequences. Or, moderate probability, moderate level of consequences.	**Medium**
4	Highly probable, moderate level of consequences. Or, moderate probability, high consequences.	**High**

5	Highly probable, high consequences.	

Appendix G: Traffic Light Protocol



Traffic Light Protocol, Version 1.0

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules.	TLP:WHITE information may be distributed without restriction.

Appendix H: Security Awareness for Aviation Sector (Prescribed by ICAO)

Learning objectives:

By the end of this course, students are expected to:

1. Develop a baseline understanding of cybersecurity;
2. Describe the most important concepts linked to this domain;
3. Appraise the interrelationships among the different elements that comprise a cybersecurity systems within civil aviation including security domains, enterprise systems, organization policies, and people;
4. Communicate risks and vulnerabilities facing the operating environment and provide examples; and
5. Contrast the various mitigation strategies and formulate a tailored an approach for risk mitigation.

Key Modules:

1. Introduction to Cyber: Overview of applicable cyber definitions, stakeholders, and policies
2. Cyber Risk Picture: Aviation security environment
3. Cyber Threat Scenarios: Threat actors and attack paths
4. Cyber Risk Management: Risk mitigation strategies to reduce risk and exposure to cyber attacks
5. Cyber and Next Steps: Where to go from here

Content of the course

I. Introduction to Cyber
   a. Definitions and Concepts
      i. Cyber: What is it?
      ii. Cyber: How does it apply to you?
      iii. Cyber and the Aviation Security Stakeholder

II. Cyber Risk Picture for the Aviation Security Environment
   a. Securing the Aviation Environment: a map
   b. Attack Methods and Connectivity between Domains
      i. Air Traffic Management (ATM)
      ii. Aircraft Systems
      iii. Airport Infrastructure
   c. Vulnerabilities and Scenarios
   d. Risk Analyses

III. Cyber Threat Scenarios and Typology
   a. Threat Actors (e.g. internal and external)
   b. Motivation

c. Intent and Objectives

IV. Cyber Risk Management

a. Individual Controls

b. Collective [Organizational] Measures

c. Respond to Events

d. Incident Reporting and Recovery Process

V. Cyber: Next Steps

a. Regulation and Legislation

i. ICAO Annex References, Risk Context Statement

ii. Regional and National Regulations

iii. Cybersecurity Guidelines (e.g. NIST, ISO)

b. Learn More

Appendix I: Choosing the right Cyber Insurance Policy

All policies have a set of exclusions, terms and definitions. Understanding these is important, so here are some additional questions to consider and help you make the right decision.

1. What security controls can you put into place that will reduce the premium?
2. Will you have to undertake a security risk review of some sort?
3. What is expected of you to reduce or limit the risks?
4. Will you get a reduction for each year you do not claim?
5. What assistance is provided to improve information governance and information security?
6. What and how big a difference to your future premiums will a claim make?
7. What support if any will be provided to assist in making the right security decisions for the industry / business you are in?
8. The security / protection industry is very fast changing, how can the insurance ensure that your policy is current?
9. Do all portable media/computing devices need to be encrypted?
10. What about unencrypted media in the care or control of your third-party processors?
11. Are malicious acts by employees covered?
12. Will you have to provide evidence of compliance to existing Data Protection Principles, in relation to your actual processing, to prove you were not acting disproportionately?
13. Although ignorance of the law is no excuse, we are just not able to keep up with all the compliance issues that may affect all the territories our company works in, would you refuse a claim if you were processing data that may contravene laws in one country but not another – because insurance policies often stipulate that you must not be breaking the law?
14. What if there is uncertainty around whether the incident took place a day before the cover was in place or on the day?
15. Are the limits for expenses grouped together in a way that the maximum limit that is covered is likely to be achieved very quickly, unless you increase the cover?
16. Are all and any court attendances to defend claims from others covered?
17. Could you claim if you were not able to detect an intrusion until several months or years have elapsed, so you are outside the period of the cover, (as with the Red October malware which was discovered after about five years)?

References

The research for this guidelines have entailed reviewing and referencing a number of publicly available documents on the internet as well as IATA Aviation CS Toolkit. We have made efforts to credit the source, where possible. Following is a non-exhaustive list of the reference documents:

1. National Information Assurance Policy – Q-CERT, MOTC
2. National Information Assurance Framework – Q-CERT, MOTC
3. IATA Aviation Cyber Security Toolkit - IATA
4. A Framework for Aviation Cyber Security – AIAA
5. Cyber Security and Risk Assessment Guideline – CANSO
6. Guide to Cyber Threat Information Sharing – NIST 800-150
7. Latham and Watkins: White Paper on Cyber Insurance
8. CSFI ATC (Air Traffic Control) Cyber Security Project, July 2015
9. Personal Data Privacy Protection Law, Qatar

32%
ECURITY BREACH