JYX JYVÄSKYLÄN YLIOPISTO UNIVERSITY OF JYVÄSKYLÄ

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Salmenpää, Tomi

Title: Information Security Governance in Civil Aviation

Year: 2022

Version: Accepted version (Final draft)

Copyright: © 2022 The Author(s), under exclusive license to Springer Nature Switzerland AG

Rights: In Copyright

Rights url: http://rightsstatements.org/page/InC/1.0/?language=en

Please cite the original version:

Salmenpää, T. (2022). Information Security Governance in Civil Aviation. In M. Lehto, & P. Neittaanmäki (Eds.), Cyber Security : Critical Infrastructure Protection (pp. 315-336). Springer. Computational Methods in Applied Sciences, 56. https://doi.org/ 10.1007/978-3-030-91293-2_13

Information Security Governance in Civil Aviation

Tomi Salmenpää

University of Jyväskylä, tomi.salmenpaa@protonmail.com

Abstract This chapter focuses mainly to proactive means in information security and more specifically governance of information security in civil aviation. The reason is that, to find sustainable, coherent and holistic way to implement information security through the complete civil aviation ecosystem, the governance plays a key role when creating sufficient framework enabling information security by design environment. The study will help aviation and other critical infrastructure sectors to consider, understand and coordinate the information security governance. The study will test how to apply information security governance with ISO27014 through such a safety critical, interconnected infrastructure sector like civil aviation.

Keywords: Cybersecurity governance, information security governance, aviation cybersecurity, aviation information security

1 Introduction

Civil aviation is a continuously evolving ecosystem in which information security plays a key role in ensuring public and societal trust and confidence in civil aviation. Other critical components, in addition to information security, are aviation safety and aviation security. Appropriate and proportionate information security measures will make sure and continuously enhance aviation safety, aviation security, and operational resilience. Information security and the governance are generally well recognized and understood at organizational level, but the role of information security governance in civil aviation at higher levels like state or international, has not yet been widely discussed. All considerations in this study represent author´s personal interpretation and expertise in this aviation cyber- security field.

1.1 Information Security Management

Reliably functioning critical infrastructure is necessity in the modern society. Continuously increasing complexity and connectivity of critical infrastructure systems increase the risk for information security threats and put the nation's

security, economy, and public safety and health, just some most important things to mention, at risk. This chapter studies one critical infrastructure sector, civil aviation, information security governance in order to support civil aviation stakeholders' coordinated and common efforts to build holistic, standardized system of system approach to civil aviation information security. Information security must have a goal, purpose.

This chapter approaches the information security and its governance by trying to ensure the operational resilience, civil aviation security and safety. In order to have coherent, holistic balanced information security management over the complete civil aviation ecosystem, the comparison is made by using different levels in aviation with relevant industry standard for governance of information security (ISO/IEC, 2013). The levels are organizational, state, regional (Europe), and international levels. Civil aviation organizations are understood to consist of all aviation domains, e.g., Air Navigation Service Providers (ANSP), Aerodrome (ADR), Airworthiness (AIR), Flight Operations (OPS), manufacturers, in other words, all aviation organizations. Other levels are state, regional (Europe) and international, for which the ISO 27014 definitions, concepts and principles are tested, because the standard itself is to improve information security management primarily within the context of the individual organization and not for higher level, like state, regional or international.

The governance is selected as the subject in the chapter, because before setting up information security actions or measures, it is fundamental to understand the objectives that one is pursuing with information security. The information security governance is discovered in the light of well-known industry standards. Because these industry standards are generally accepted and matured as the best practices by the information security industry, community and stakeholders, they provide a solid ground to apply those standards for civil aviation purposes. Then the current civil aviation existing management and governance frameworks are described, and information security governance definitions, concepts and principles are projected to those existing governance models.

In this chapter, the differences between information security and cybersecurity are not so great as to cause a problem. So the differences are therefore ignored. At the very beginning, the terms information security and management system need to be defined and understood. Information security means preservation of confidentiality, integrity and availability of information whereas the management system as for a set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives (ISO/IEC, 2017). Together they are Information Security Management System (ISMS) that consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.

The National Institute of Standards and Technologies (NIST) has issued a cybersecurity framework for improving critical infrastructure cybersecurity, that

provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk (NIST, 2018).

The cybersecurity framework describes five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover (Table 1). They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. When considered all together, these functions provide a high-level strategic lifecycle for an organization's management of cybersecurity risk. The framework core then identifies underlying key categories and subcategories for each function, and matches them with example informative references such as existing standards, guidelines, and practices for each subcategory (NIST, 2018).

Table 1. Function and category unique identifiers (NIST, 2018)

Function unique identifier	Function	Category unique identifier	Category
ID	Identify	ID.AM	Asset management
		ID.BE	Business environment
		ID.GV	Governance
		ID.RA	Risk assessment
		ID.RM	Risk management strategy
		ID.SC	Supply chain risk management
PR	Protect	PR.AC	Identity management and access control
		PR.AT	Awareness and training
		PR.DS	Data security
		PR.IP	Information protection processes and procedures
		PR.MA	Maintenance
		PR.PT	Protective technology
DE	Detect	DE.AE	Anomalies and events
		DE.CM	Security continuous monitoring
		DE.DP	Detection processes
RS	Respond	RS.RP	Response planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery planning
		RC.IM	Improvements
		RC.CO	Communications

The Identify function means: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify function are foundational for effective use of the framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts consistent with its risk management strategy and business needs. Examples of outcome categories within this function include: Asset management, Business environment, Governance, Risk assessment, and Risk management strategy (NIST, 2018). This chapter researches the information security governance and its meaning in the whole aviation ecosystem.

1.2 Governance in Information Security Management

Governance means many things depending on the context or discussion. In general, governance comprises all of the processes of governing – whether undertaken by the government of a state, by a market or by a network – over a social system (family, tribe, formal or informal organization, a territory or across territories) and whether through the laws, norms, power or language of an organized society (Bevir, 2012). In this chapter the governance is discussed from the information security management perspective at various levels, referring to existing industry standards in information security.

In information security and standard such as ISO/IEC 27014, the governance of information security is defined as a system by which an organization's information security activities are directed and controlled (ISO/IEC, 2013). NIST framework describes the governance in the following way: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the organization management of cybersecurity risk (NIST, 2018). In reality, it is widely understood that for organizations it is impossible to protect everything in the cyberspace and they need to make prioritization. Therefore, information security risk management plays a key role defining organization assets that have value for organization or their stakeholders.

In order to make appropriate information security management in place, it is crucial to consider and understand the objectives of information security governance. In the standard ISO/IEC (2013) it is defined:

- align the information security objectives and strategy with business objectives and strategy (strategic alignment),
- deliver value to the governing body and to stakeholders (value delivery),
- ensure that information risk is being adequately addressed (accountability).

The governance is important to understand at different levels in aviation and cybersecurity because the different levels should have converging strategies in aviation cybersecurity and governance plays a fundamental role to set right policies

always down to practical solutions in aviation information security. In addition, between the aviation organizations there should not be gaps, duplication or uncoordinated areas in this chain of aviation cybersecurity governance.

In this chapter, information security governance is researched from the civil aviation ecosystem perspective at four different levels: organization, national, regional, and international. At individual organization level the information security objectives and strategy are aligned with the business objectives and strategy of that organization. At national level in civil aviation these information security objectives and strategy are different from those at organization level. It is the whole national and collectively international aviation system resiliency, safety and security, where information security objectives and strategy are aligned. Eventually at the broadest levels, regional (Europe) and international level, civil aviation information security objectives and strategy are different because the business objectives and strategy are different from those at national and organizational levels. Evaluating these differences can give an opportunity to better understand information security governance and make development according the needs, for example, when digitizing organization, society, or the whole ecosystem.

Comparing the term "system" in ISO/IEC (2013), it has different meaning in information security at different levels (organizational, national, regional, and international). Also, the alignment of the information security objectives and strategy with business objectives and strategy varies because the

- information security objectives and strategy are different at every level;
- business objectives and strategy are different at every level.

In aviation, the governance at international level means all of the processes undertaken by international organization who has the necessary mandate or role to be able to govern civil aviation. The governance means all of the processes that comes to civil aviation. At state level, governance of aviation is different thing. The scope of processes is different and they are undertaken by government of a state according to a system in that society. In organization, the processes in aviation governance are again different and means the collection of mechanisms, processes and relations used by various parties to control and to operate organizations. Organization governance includes the processes through which organizations objectives are set and pursued in the context of the social, regulatory and market environment.

2 Information Security Management in Civil Aviation

This section focuses on efficient information security management in civil aviation in order to ensure operational resiliency, secure and safe civil aviation system. That means the information security and its management needs to be considered in the light of the overall civil aviation safety and security management.

Aviation security and safety management fundamentally complement each other. While aviation security experts often hold coordination links to threat information sources and are used to dealing with intentional threats and the respective methodologies, aviation safety experts have extensive know-how of the consequences on the safety of flight in case of system failure and know the design and set-up of systems and existing mitigation measures such as redundancies (ECAC, 2020). Due to existing strong, holistic and end-to-end (from the policy to practice) security and safety governance framework in civil aviation, it is strongly recommended to implement information security to the existing safety and security management frameworks.

International policies and standards in civil aviation are coordinated through the International Civil Aviation Organisation (ICAO). ICAO is specialized agency of the United Nations (UN), which is directed and endorsed by the governments. In ICAO, also industry, society groups, and other regional and international organizations participate in the exploration and development of new standards. In sector such as civil aviation where flying aircraft, commonly used processes and protocols do not recognize borders, it is paramount to have international and standardized approach in all areas of aviation safety and security.

2.1 Concept of Safety Management in Civil Aviation

First, it is paramount to understand the meaning of civil aviation safety management. Civil aviation safety management is commonly understood as a set of principles, framework, processes and measures to prevent accidents, injuries and other adverse consequences that may be caused by using service or product. The objective of safety management in the aviation industry is to prevent human injury or loss of life and to avoid damage to the environment and to property (SKYbrary, 2020). Safety Management System is the formal, top-down, organization-wide approach to managing safety risk and ensuring the effectiveness of safety risk controls. It includes systematic procedures, practices, and policies for the management of safety risk (FAA, 2020).

In aviation, there is traditional, strong, ecosystem-based and standardized safety governance concept in place. In that concept, the global chain of safety management plays a key role, where, at international level, the ICAO's Global Aviation Safety Plan (GASP) presents the strategy that supports the prioritization and continuous improvement of aviation safety. The GASP, along with the Global Air Navigation Plan (GANP), provides the framework in which regional and national aviation safety plans will be developed and implemented, thus ensuring harmonization and coordination of efforts aimed at improving international civil aviation safety, capacity, and efficiency (ICAO, 2016; ICAO, 2019a).

At regional level in Europe, European Plan for Aviation Safety (EPAS) constitutes the regional aviation safety plan for European Aviation Safety Agency (EASA) member states. The EPAS set out the strategic priorities, strategic enablers

and main risks affecting the European aviation system and the necessary actions to mitigate those risks and further improve aviation safety.

The EASA member states have their own State Safety Programs (SSPs), which is the detailed level national description of their safety management system. They follow the ICAO's GASP and the European EPAS accordingly, but also maintain and improve them by feeding important, e.g., safety performance information to those programs.

The aviation organizations have their Safety Management Systems (SMS) to meet these safety risk management requirements and safety performance objectives. It is noteworthy that SMS requirements are not yet applicable for all aviation domains, but the most critical ones, like airlines, are mandated to have SMS.

2.2 Concept of Security Management in Civil Aviation

Whereas civil aviation safety focus on reducing the likelihood of accident happening, the civil aviation security focus to safeguard international civil aviation against acts of unlawful interference. The International Civil Aviation Organization (ICAO) has the leadership role at global level to develop international policies and measures at international level. In general, this contains all acts that jeopardize the safety of civil aviation. Current global level policies and measures are well implemented against the physical acts, but both digital and physical information security are underway internationally, regionally, and nationally, including aviation organizations.

Aviation security in the aviation community generally means all unlawful interference against civil aviation. Such acts or attempts jeopardize the safety of civil aviation (ICAO, 2020). The unlawful interference of civil aviation is safe guarded by the commonly agreed norms starting from the international level. Information security is defined as protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (NIST, 2018).

In theory, the difference between unlawful interference compared to unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability is not that great. In practice, there is a grey area because it depends on the impact of information security incident in aviation security or safety. Information security incident not always impacts aviation in a way that is defined as unlawful interference, but still the incident can seriously compromise the public trust or confidence in civil aviation.

In aviation security, there is also a strong and standardized security governance concept in place. ICAO Global Aviation Security Program (GASeP) addresses the needs of states and industry in guiding all aviation security enhancement efforts. The objective of the GASeP is to help ICAO, states and aviation stakeholders

enhance the effectiveness of global aviation security. The GASeP seeks to unite the international aviation security community and inspire action in this direction, taking into account that the threats and risks faced by the civil aviation community continue to evolve. It is also intended to achieve the shared and common goal of enhancing aviation security worldwide and to help states come together to fulfil the commitments set out in UNSCR 2309 (2016) and relevant ICAO assembly resolutions (ICAO, 2020).

The states have their National Civil Aviation Security Program (NCASP) to safeguard civil aviation operations against unlawful interference. The NCASP must meet the requirements from regulations, practices and procedures, which take into account the safety, regularity and efficiency of flights (ICAO, 2020).

2.3 Concept of Cybersecurity in Civil Aviation

The concept of cybersecurity is not yet in place compared to aviation safety and security and is still evolving at all levels, international, national and organizational levels. At international level there is published and agreed ICAO Aviation Cybersecurity Strategy and its Action Plan for the ICAO, states, and industry in aviation cybersecurity with a vision that civil aviation sector being resilient to cyber-attacks and remains safe and trusted globally whilst continuing innovate and growt(ICAO, 2019b). In the ICAO Strategy and Action Plan there are eight pillars, and one is governance. In the actions it is highlighted for the states the need to develop clear national governance and accountability for civil aviation cybersecurity. Another important action is to include cybersecurity into national aviation safety and security programs. However, more specific definitions or actions about governance and its meaning are not available in the strategy or action plan.

At regional level in Europe the information security governance in aviation is discussed in some publications. The most accurate recommendation is available in the European Civil Aviation Conference (ECAC) guidance material on cybersecurity in civil aviation (ECAC 2020), which provides important principles on the governance that states and organizations should follow in aviation cybersecurity. The principles are about roles and accountability in the civil aviation cybersecurity; however, the meaning of governance is not defined at a detailed level. In Europe, there is aviation cybersecurity strategy by the European Strategic Coordination Platform (ESCP). The ESCP Strategy for Cybersecurity in Aviation provides a systematic approach with objectives, to build in cybersecurity into civil aviation, but does not provide direct recommendations to cybersecurity governance. For organizations, the information security industry standards provide sufficient recommendations and best practices to information security governance at organizational level, e.g., ISO 27014. For all these reasons described before, this chapter is about projecting the available standards to higher levels, such as at national, regional, and international levels.

3 Information Security Management Governance in Civil Aviation

The International Organisation for Standardization (ISO) provides relevant standard for Governance of Information Security ISO 27014. In addition, NIST standards, e.g., SP 800-39 was also evaluated, but the ISO 27014 was chosen because it provided from governance perspective more prescriptive model to use and meet the goals of this study. Because the ISO 27014 is applicable for all types and sizes of organizations, however primarily from the individual organization context, this encouraged to test this model at higher levels too, in order to make different needs for information security governance meaning and more tangible.

3.1 Definitions

To make the comparison from organization level to state or higher levels, there are some important definitions in ISO 27014 (Table 2) which need to be first translated and understood from that respective level. When these definitions are translated to higher levels, at state level there are sufficient ground available for cybersecurity (Table 3).

Table 2. Definitions in ISO 27014

Definitions	Meaning at organization level
Executive management	Delegated responsibility from the governing body for implementation of strategies and policies to accomplish the purpose of the organization
Governing body	Accountability for the performance and conformance
Governance of information security	System by which an organization's information security activities are directed and controlled - Organization Management System
Stakeholder	Any person or organization that can affect, be affected by, or perceive themselves to be affected by an activity of the organization

Table 3. Definitions at state level

Definitions	Meaning at national level
Executive management	Agencies and authorities for aviation security and safety
Governing body	Ministries, agencies and authorities for aviation security and safety
Governance of information security	National civil aviation security and safety programs
Stakeholder	Any person or organization that can affect, be affected by, or perceive themselves to be affected by an activity of the agencies and authorities - Regional management system

Table 4. Definitions at regional level

Definitions	Regional (Europe) level
Executive management	DG MOVE, DG HOME, DG CONNECT, EASA
Governing body	European Commission
Governance of information security	European Aviation Safety (EPAS) and security (?) programs
Stakeholder	Any person or organization that can affect, be affected by, or perceive themselves to be affected by an activity of the agencies and organizations

Table 5. Definitions at international level

Definitions	International level
Executive management	ICAO & member states
Governing body	ICAO & member states
Governance of information security	Global Aviation Safety Plan (GASP) and Global Aviation Security Plan (GASeP)
Stakeholder	Any person or organization that can affect, be affected by, or perceive themselves to be affected by an activity of the agencies and organizations

At regional level, e.g., in Europe, things will get more interesting. Executive management and governing body are available in the European governance model, but the system by which a regional-level information security activity is directed and controlled, does not meet the ISO 27014 recommendations (Table 4). In Europe, the EPAS provide in aviation safety the needed system, but in the aviation security there is no relevant system available.

The international level has sufficient systems available, but the ICAO GASeP does not sufficiently recognize information security in its full spectrum (Table 5). The GASeP is more focused to unlawful interference of civil aviation recognize well, e.g., traditional terrorist threats. In the information security the threat actors are, however, very different, e.g., nation state, cybercriminals, hacktivists, terrorist groups, and insiders. The method to handle information security threat actors needs to be reviewed and coordinated in the GASeP. At international level, the GASP and GASeP can provided sufficient system for information security.

3.2 Concepts

Governance of information security needs to align objectives and strategies for information security with business. The governing body is ultimately accountable for an organization's decisions and the performance of the organization. In respect to information security, the key focus of the governing body is to ensure that the organization's approach to information security is efficient, effective, acceptable and in line with business objectives and strategies giving due regard to stakeholder expectations (ISO/IEC, 2013). This applies to all levels, aviation organizations, state agencies and authorities, regional and international levels.

Next, the objectives and desired outcomes of the information security are projected at different levels. For the aviation organizations defining information security objectives and desired outcomes is straight forward work respect to the ISO 27014 (Table 6). For the state, regional and international level, there is already a solid governance model in civil aviation safety and security as previously described where information security should be implemented. From that perspective, the following objectives and desired outcomes are available in the available aviation cybersecurity strategies (ICAO and ESCP) (Table 7).

Table 6. Objectives and desired outcomes for aviation organization

Concepts	Meaning at organizational level
Governance objectives of information security 1) align the information security objectives and strategy with business objectives and strategy (strategic alignment) 2) deliver value to the governing body and to stakeholders (value delivery) 3) ensure that information risk is being adequately addressed (accountability)	1) Business objectives: aviation organization specific 2) Value delivered: aviation organization specific
Desired outcomes from effectively implementing governance of information security include 1) governing body visibility on the information security status 2) an agile approach to decision-making about information risks 3) efficient and effective investments on information security 4) compliance with external requirements (legal, regulatory or contractual)	Indicators (need to be defined) how well the governance objectives are met: Organization management system and performance metering (indicators) from the relevant maturity metering models & information security standards (Traficom, 2020)
Relationship with other areas of governance models (a holistic and integrated governance model with information security management usually benefits the governing body)	Governance of safety, security, legislations, information technology and business objectives

Table 7. Objectives and desired outcomes at state, regional and international levels

Concepts	Meaning
Governance objectives of information security: 1) align the information security objectives and strategy with business objectives and strategy (strategic alignment) 2) deliver value to the governing body and to stakeholders (value delivery) 3) ensure that information risk is being adequately addressed (accountability)	1) Business objectives & strategy: Efficiently ensure public trust & confidence, operational resilience, safety and security in the digital society and aviation 2) Value delivered To governing body: timely information about industry information security (for safety and security) capability and risks -> the information ensures sufficient regulatory framework, procedures, and processes in information security. To stakeholders: holistic, standardized performance and risk-based legal framework, procedures and processes
Desired outcomes from effectively implementing governance of information security include 1) governing body visibility on the information security status 2) an agile approach to decision-making about information risks 3) efficient and effective investments on information security 4 compliance with external requirements (legal, regulatory or contractual)	Indicators (need to be defined) how well the governance objectives are met: State, regional, and international aviation safety and security programs and their indicators
Relationship with other areas of governance models (a holistic and integrated governance model with information security management usually benefits the governing body)	Coherence in aviation safety, aviation security, and information security management governance

3.3 Principles

Meeting the needs of stakeholders and delivering value to each of them is integral to the success of information security (ISO/IEC, 2013). There are six principles in ISO 27014 to achieve the governance objective of aligning information security closely with the goals of the business and delivering value to stakeholders:

Principle 1: Establish organization-wide information security;
Principle 2: Adopt a risk-based approach;
Principle 3: Set the direction of investment decisions;
Principle 4: Ensure conformance with internal and external requirements;
Principle 5: Foster a security-positive environment;
Principle 6: Review performance in relation to business outcomes.

These principles of information security governance were the most challenging to project and compare for the perspective levels.

The principles provide a good foundation for the implementation of governance processes for information security. The statement of each principle refers to what should happen, but does not prescribe how, when, or by whom the principles would be implemented, because these aspects are dependent on the nature of the organization implementing the principles. The governing body should require that these principles be applied and appoint someone with responsibility, accountability, and authority to implement them (ISO/IEC, 2013).

3.3.1 Principles at Aviation Organizational Level

Principles at aviation organizational level can be directly transferred from the standard. The business and value delivery in this study are focused to operational resiliency, aviation security and safety. With these values the principles can be defined in the following way.

Principle 1: Establish organization-wide information security
For aviation organization, information security activities should be comprehensive and integrated with aviation safety and security. This principle emphasize the need of information security to be integrated to all aviation security and safety policies, processes, procedures and technologies. Information security responsibility and accountability should be established across the full span of organisation´s activities, including aviation safety and security.

Principle 2: Adopt a risk-based approach
Governance at organizational level should be based on risk-based decisions. Determining how much security is acceptable should be based upon the risk appetite of an organization, including loss of competitive advantage, compliance and liability risks, operational disruptions, reputational harm, and financial loss. (ISO/IEC, 2013). In such interdependent ecosystem like civil aviation, the minimum level of information security risk appetite for aviation safety and security is based on compliance and liability through the evolving legislation. In addition in aviation, the organization and their aviation services, governance of information security should be based on consistent and integrated risk management including aviation safety, aviation security, and information security.

Principle 3: Set the direction of investment decisions
To optimize information security investments to support organizational objectives in aviation organizations, governance of information security should establish an information security investment strategy based on business outcomes achieved, resulting in harmonization between business and information security requirements and thereby meeting the current and evolving needs of stakeholders (ISO/IEC 2013). When the information security management from the operational resilience, aviation safety, and aviation security perspectives is implemented comprehensively and consistently in the aviation organizations, it enables controlled investment decisions and gives an opportunity for optimized investments, too.

Principle 4: Ensure conformance with internal and external requirements
For aviation organizations, governance of aviation information security should ensure that information security policies and practices conform to relevant mandatory legislation and regulations, as well as committed business or contractual requirements and other external or internal requirements. To address conformance and compliance issues, the governing body should obtain assurance that information security activities are satisfactorily meeting internal and external requirements by commissioning independent security audits (ISO/IEC, 2013). Current legislative framework in all levels; state-, regional and international levels is strongly evolving, meaning information security management is being implemented into aviation safety and security management. Organizations should follow closely the development of this legislative framework. The business and contractual requirements also need to be emphasized, because very likely they cover more specific, but converging information security requirements with the evolving legislative framework.

Principle 5: Foster a security-positive environment
In aviation organization, governance of aviation information security should be built upon human behavior, including the evolving needs of all the stakeholders, since human behavior is one of the fundamental elements to support the appropriate level of information security. If not adequately coordinated, the objectives, roles, responsibilities, and resources may conflict with each other, resulting in the failure to meet business objectives. Therefore, harmonization and concerted orientation between the various stakeholders is very important. To establish a positive aviation information security culture, the governing body should require, promote, and support coordination of stakeholder activities to achieve a coherent direction for aviation information security. This will support the delivery of security education, training, and awareness programs (ISO/IEC, 2013).

Principle 6: Review performance in relation to business outcomes
In aviation organizations the governance of information security in aviation should ensure that the approach taken to protect aviation information is fit for purpose in supporting the organization, providing agreed levels of information security. Security performance should be maintained at levels required to constantly meet current and future business requirements. To review performance of information security from a governance perspective, the governing body should evaluate the performance of information security related to its business impact, not just effectiveness and efficiency of security controls. This can be done by performing mandated reviews of a performance measurement program for monitoring, audit, and improvement, and thereby link information security performance to business performance (ISO/IEC, 2013). Performance measurement program is an important enabler also to make efficient investments on information security.

3.3.2 Principles at State Level

Principles at state level can be derived from the standard by changing the angle of view to state level. It is important to understand the differences especially in responsibilities. The state and the relevant agencies and authorities are responsible for the society, national aviation system safety and security to general public and all stakeholders.

Principle 1: Establish state-wide information security in civil aviation
At state level, civil aviation safety, aviation security, and information security agencies and authorities should co-operate closely for aviation eco-system wide information security, meaning the governance at state level ensure that information security activities are comprehensive and integrated to aviation safety and security. It is important to establish responsibility and accountability for information security for aviation safety, security and society.

Principle 2: Adopt a risk-based approach
In information security for aviation safety and aviation security, the risk appetite at state level is bound to compliance and liability with regional and international aviation legislation. Also, the societal responsibility of ensuring state aviation system is operational in all circumstances, affect risk appetite. Since the aviation information security legislation is strongly risk-based, it can be challenging to define how much information security is acceptable. Therefore it is paramount at state level to have good understanding of the overall risk picture, in order to perform state level role in civil aviation: guide, regulate and oversight aviation organizations some to mention. At state level the overall civil aviation risk picture could be part of the national civil aviation safety (State Safety Programme - SSP) and security (National Civil Aviation Security Program - NCASP) programs. That will help states and their stakeholders to better understand aviation ecosystem wide risks. Since the governance of information security should be based on risk-based decisions with an overall risk profile of the state, the state is better able to determine how much information security is acceptable in the risk-based world. This helps states consider their willingness to take risks. In addition to risk appetite, the state also need to make sure the governance of information security is based on aligned and integrated risk-based approach, meaning information security is integrated in aviation safety (SSP) and security (NCASP).

Principle 3: Set the direction of investment decisions
For the states, this principle means governance of information security could establish an aviation information security investment strategy based on aviation business, safety and security outcomes achieved, both in short and long term, thereby meeting the current and evolving needs of society and stakeholders. To enable information security investments to support national and international civil aviation objectives, the national aviation governing body should consider too that information security is integrated with existing civil aviation processes for capital and operational expenditure. This is very important aspect especially in the modern

digitized society and aviation ecosystem. If information security is not coordinated through all levels, that can lead to deficiencies in the implementation of information security, in investments and high and ineffective development and operating costs in civil aviation.

Principle 4: Ensure conformance with internal and external requirements
At state level in civil aviation, there is strong and evolving framework in aviation safety and security, where information security will be implemented. Information security governance at state level should ensure the state information security policies and practices conformance with the relevant domestic, regional and international legislation and regulations, as well as with the operational or contractual requirements or other external or internal requirements. To address conformance and compliance issues, the governing body at state level should obtain assurance that information security activities are satisfactorily meeting internal and external requirements by commissioning independent security audits.

Principle 5: Foster a security-positive environment
Governance of aviation information security at state level should be built upon human behavior, including the evolving needs of all the stakeholders, since human behavior is one of the fundamental elements to support the appropriate level of information security. The human behavior is a strong asset in aviation, because there is existing strong safety and security culture, which can be leveraged into information security as well. At state level, the agencies and authorities are in the key role to stakeholders domestically or abroad, fostering the security-positive environment. If the human behavior is not adequately coordinated, the objectives, roles, responsibilities, and resources may conflict with each other, resulting in the failure to meet eventually the operational objectives. Therefore, harmonization and concerted orientation between the various stakeholders is very important. To establish a positive aviation information security culture, the governing body (relevant state agencies and authorities) should require, promote, and support coordination of stakeholder activities to achieve a coherent direction for aviation information security. This will support the delivery of security education, training, and awareness programs.

Principle 6: Review performance in relation to operational outcomes
For the states, governance of information security in aviation should ensure that the approach taken to protect aviation information at state level is fit for purpose in supporting the organizations, providing agreed levels of information security. Security performance at state level should be maintained at levels required to meet current operational and societal requirements. To review performance of information security in aviation at state level from a governance perspective, the governing body (relevant agencies and authorities) should evaluate the maturity of aviation information security related to its aviation operational resiliency, safety, and security impact, not just effectiveness and efficiency of security controls. If this principle is not identified, that can provide fallacy between theory and practice in the aviation information security. This can be done by performing mandated

reviews of a performance measurement program for monitoring, audit, and improvement, and thereby link information security performance to operational performance.

3.3.3 Principles at Regional Level (Europe)

Principles at regional level can be defined by considering the responsibilities of European civil aviation governing body and relevant European agencies, who are responsible for the European aviation system information security, safety and security.

Principle 1: Establish Regional-wide information security in civil aviation
Regional level aviation safety and security agencies and information security agency should establish aviation eco-system wide information security. In Europe this means the governance at European level should ensure that information security activities are consistently and comprehensively integrated to aviation safety and security. To establish European level aviation information security, the responsibilities and accountabilities should be defined and established across the full span of European civil aviation activities. This is an important principle requiring all, the European civil aviation governing body and executive management in safety, security, and information security, seamlessly cooperate and coordinate information security in aviation safety and security.

Principle 2: Adopt a risk-based approach
In information security for aviation safety and security, the risk appetite at regional level could be defined similarly like at state level. It is bound to compliance and liability with international aviation legislation, but overall understanding of information security risks is paramount to assure risk-based legislation. Also at regional level the governance of aviation information security should be based on aligned and integrated risk-based approach, meaning information security is integrated in the aviation safety (European Plan for Aviation Safety) and security. It is important to however note, that currently there is no European aviation security program. Instead, there are common rules and basic standards for the states and industry on aviation security and the procedures to monitor the implementation of the common rules and standards, which are implemented by the states through the NCASP.

Principle 3: Set the direction of investment decisions
The principle at regional level is the same as at state and international levels.

Principle 4: Ensure conformance with internal and external requirements
Governance of the European level aviation information security should ensure that European civil aviation information security policies and practices conform to relevant mandatory international legislation and regulations, as well as committed business or contractual requirements and other external or internal requirements. To address conformance and compliance issues, the governing body in Europe should

obtain assurance that information security activities are satisfactorily meeting internal and external requirements by commissioning independent security audits. The independent audit or relevant action would be beneficial to give an objective and comprehensive view, how well the European system currently and in the future meets the internal and external requirements.

Principle 5: Foster a security-positive environment

At regional level, governance of aviation information security at European level should be built upon human behavior, including the evolving needs of all the stakeholders, since human behavior is one of the fundamental elements to support the appropriate level of information security. The human behavior is a strong asset in aviation, because there is existing strong safety and security culture, which can be leveraged into information security as well. The European agencies and authorities are in the key role to stakeholders regionally, fostering the security-positive environment. When sufficiently coordinated, the objectives, roles, responsibilities, and resources converge with each other, resulting efficiently to meet operational objectives. Therefore, harmonization and concerted orientation between the various stakeholders, European and non-European states and stakeholders, is very important. To establish a positive aviation information security culture, the governing body (European Commission) should require, promote and support coordination of stakeholder activities to achieve a coherent direction for aviation information security. This will support the delivery of security education, training, and awareness programs. The existing aviation safety and security education -, training and awareness framework provides a good opportunity to convey information security training to aviation.

Principle 6: Review performance in relation to operational outcomes

At regional level in Europe, governance of information security in aviation should ensure that the approach taken to protect aviation information at European level is fit for purpose in supporting the organizations, providing agreed levels of information security. Security performance at European level should be maintained at levels required to constantly meet current and future operational requirements. To review performance of information security in aviation at European level from a governance perspective, the governing body (European Commission) should evaluate the performance of aviation information security related to its societal, operational resilience, safety and security impact, not just effectiveness and efficiency of security controls. This can be done by performing reviews of a performance measurement program for monitoring, audit, and improvement, and thereby link information security performance to operational performance in aviation.

3.3.4 Principles at International Level

Principles at international level can be defined by considering the responsibility of civil aviation governing body at international level, who is responsible for the international civil aviation information security, safety, and security governance.

Principle 1: Establish international-wide information security in civil aviation
At international level, aviation information security activities should be consistent and comprehensive and integrated with all aviation safety, security, and civil aviation activities. To establish the international level wide civil aviation information security, the responsibility and accountability for civil aviation information security for aviation safety and security, should be established across the full span of international civil aviation activities. This principle is supported by the ICAO Aviation Cybersecurity Strategy and Action Plan.

Principle 2: Adopt a risk-based approach
Similarly with the regional and state levels, the governance of information security should be based on risk-based decisions. The risk appetite determining how much information security is acceptable, should be based on the risk appetite consensus by the states and industry, including operational disruptions, reputational harm, financial loss or loss of public trust and confidence. In addition, the governance of information security should be based on aligned and integrated risk-based approach in information security, aviation safety and security. At international level, key enabler for this principle is integrated information security in the global aviation safety (GASP) and security programmes (GASeP).

Principle 3: Set the direction of investment decisions
The principle at international level is the same as at state and regional levels.

Principle 4: Ensure conformance with internal and external requirements
At the highest level, international level, it is the international aviation community, states and industry together who are developing and implementing civil aviation information security policies and practices into civil aviation. Therefore, there are no relevant mandatory legislation and regulations that information security policies and practices at international level should conform.

Principle 5: Foster a security-positive environment
The same way with regional level, the governance of aviation information security at international level should be built upon human behavior. The human behavior is a strong asset in aviation due to existing strong safety and security culture, which can be leveraged into information security as well. At international level, states and industry through ICAO, are in the key role to foster security-positive environment. Sufficiently coordinated, the objectives, roles, responsibilities, and resources converge with each other, resulting efficiently to meet operational objectives. Harmonization and concerted orientation between the various stakeholders is very important. To establish a positive aviation information security culture, the governing body (ICAO) should establish, require, promote and support

coordination of stakeholder activities to achieve a coherent direction for aviation information security. This will support the delivery of security education, training, and awareness programs. The existing aviation safety and security education -, training and awareness framework provides a good opportunity to convey information security training to aviation.

Principle 6: Review performance in relation to operational outcomes
At international level, governance of information security in aviation should ensure that the approach taken to protect aviation information at international level is fit for purpose in supporting the states and aviation organizations (industry), providing agreed levels of information security. Security performance at international level should be maintained at levels required to constantly meet current and future operational requirements. To review performance of information security in aviation at international level from a governance perspective, the governing body (ICAO) should evaluate the performance of aviation information security related to its operational impact, not just effectiveness and efficiency of security controls. This can be done by performing reviews of a performance measurement program for monitoring, audit, and improvement, and thereby link information security performance to operational performance.

4 Conclusions

The information security management is generally well recognized in the civil aviation. However, the significance and meaning of information security governance need some attention. This study focuses on information security governance through ISO 27014 definitions, concepts, and principles at different levels in the civil aviation. In order to make sustainable and efficient aviation information security management, the meaning and objectives of information security governance should be better recognized and understood, because it is crucial for efficient performance and risk-based information security regardless of the respective level.

The objective of this study was to test and evaluate how to apply relevant standard in information security governance in civil aviation and at different levels. The study address that the ISO 27014 definitions, concepts and principles can be applied to higher levels than organizational level. No obstacles were found for the application and important information security governance objectives, desired outcomes and principles were recognized for different levels. The ISO 27014 is dedicated to ISMS in the context of organization and can be applied for all types or size of organizations. This means higher levels require special consideration with the definitions, concepts, and principles. In this study, the projected definitions, concepts, and principles for the higher levels are based on the current international, regional and state level working group work in the ICAO, ECAC and ESCP, their publications and relevant industry standards in information security. The

considerations in this study represent author´s personal interpretation and expertise in this field. The author is actively involved in the relevant ICAO, ECAC and ESCP working group work, having also strong aviation safety and information security background.

The study discovered interesting aspects in information security governance which have not been properly recognized at the current international, regional, or state level aviation information security. It would be beneficial to research them and their status in more detail. It is recommended, that every organization at all levels consider their role and responsibility in the aviation ecosystem and define their information security governance at more detailed level. This study can provide one approach to help in this work.

Specific observations about the status of each principle are not presented in this study. However, it can be generally observed that there are shortages in the governance of information security in civil aviation. It is important to make sure that governing body, executive management, and governance system are available at all levels. Without those elements, it is very hard to implement sufficient information security management in civil aviation. Other observations were related to objectives and desired outcomes. At all levels, objectives and outcomes are important to define beforehand. Information security governance have also six important principles, which should be defined for all levels. This would help and ensure common effort towards consistent and coherent civil aviation information security.

References

Bevir, M. (2012). *Governance: A Very Short Introduction.* Oxford University Press.

ECAC (2020). ECAC guidance material on cyber security in civil aviation. European Civil Aviation Conference (ECAC).

FAA (2020). Safety Management System (SMS). U.S. Department of Transportation, Federal Aviation Administration (FAA), https://www.faa.gov/about/initiatives/sms/

ICAO (2016). Global Air Navigation Plan 2016–2030. Doc 9750-AN/963, Fifth ed., International Civil Aviation Organization (ICAO), https://www.icao.int/publications/Documents/9750_5ed_en.pdf

ICAO (2019a). Global aviation safety plan. Doc 10004, 2020—2022 ed., International Civil Aviation Organization (ICAO), https://www.icao.int/safety/GASP/Documents/Doc.10004%20GASP%202020-2022%20EN.pdf

ICAO (2019b). Aviation Cybersecurity Strategy. International Civil Aviation Organization (ICAO)https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf

ICAO (2020). Security: Safeguarding international civil aviation against unlawful interference. Annex 17, 11th ed., International Civil Aviation Organization (ICAO).

ISO/IEC (2013). ISO/IEC 27014:2013: Information technology, security techniques, governance of information security. International Organisation for Standardization (ISO) and International Electrotechnical Commission (IEC).

ISO/IEC (2017). ISO/IEC 27000:2017: Information technology, security techniques, information security management systems, overview and vocabulary (ISO/IEC 27000:2016). International Organisation for Standardization (ISO) and International Electrotechnical Commission (IEC).

NIST (2018). Framework for improving critical infrastructure cybersecurity. Version 1.1, National Institute of Standards and Technologies (NIST).

SKYbrary (2020). Safety management. SKYbrary, https://www.skybrary.aero/index.php/Safety_Management

Traficom (2020). Kybermittari. National Cyber Security Centre, Finnish Transport and Communications Agency Traficom, https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari