Ethical:

A list of codes that organisations adopt in understanding the difference between "wrong" and "right."

Information security auditors towards ethical:

- Procedure audit processes that believe the assessed risk level for irregular and unlawful acts
- Examine the result of the audit processes for an indication of illicit acts.

Legal:

Information security auditors will examine legal contracts for buying and selling software applications, computer equipment and services like outsourcing arrangements and Maintenance agreements.

Some of the legal contracts are employee contracts, confidentiality agreements, discovery agreements.

Social:

Information security audit must analyse, comprehend, report, and ultimately improve an organisation's social and moral interpretation. It's a method for analysing, measuring, verifying, reporting, and improving an organisation's social performance. Social auditing creates an impact on IG.

Effectiveness of the Information Security Management System. (Aldya,2019)

The problem of information security is often caused by bad management. Therefore, we need to implement a reliable information security management system at Air MSky. According to ISO 27001, ISMS implementation follows a Plan-Do-Check-Act (PCDA) model for continuous improvement in ISMS processes: (Aldya,2019)

- Plan. Identify problems and gather helpful information to evaluate security risks. Define policies and processes that can address the root causes of the problem development of methods for the continuous improvement of information security management skills.
- Do. Implement the devised security policies and procedures. The implementation follows the ISO standards, but the actual performance is based on the resources available to your company.
- Check. Monitor the effectiveness of ISMS policies and controls. Evaluate tangible outcomes as well as behavioural aspects associated with the ISM processes.
- Act. Focus on continuous improvement. Document the results, share knowledge, and use a feedback loop to address the future implementation of the PCDA model of ISMS policies and controls.

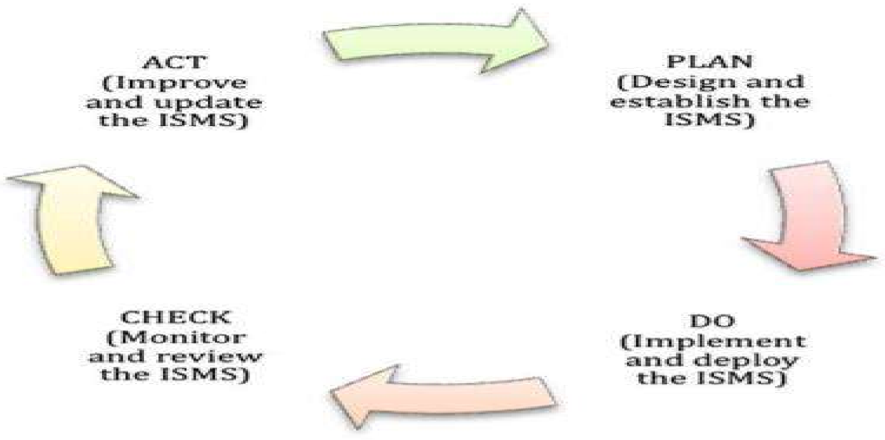
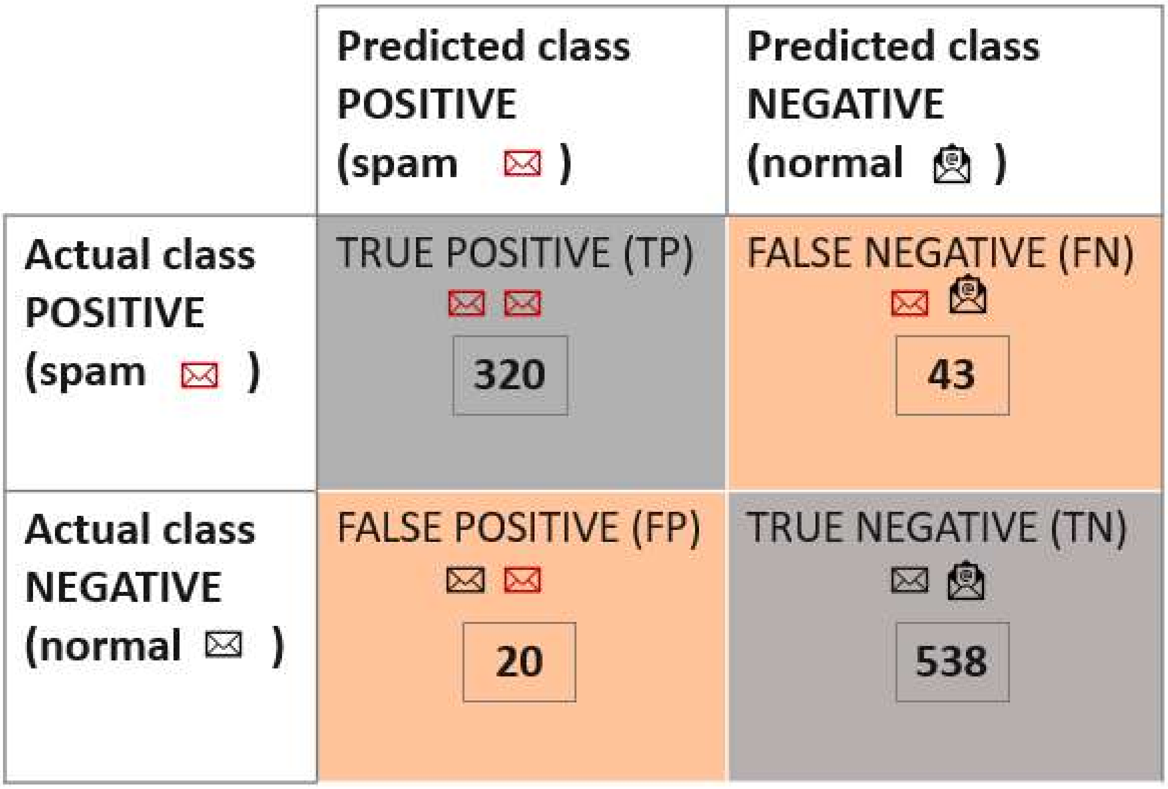

ACT (Improve and update the ISMS)
PLAN (Design and establish the ISMS)
DO (Implement and deploy the ISMS)
CHECK (Monitor and review the ISMS)

Fig 1: PDCA model source: (Humphreys,2008)

As has been described above, one of the principles approaches to the process of the ISMS (check) where the operation is made by measuring the execution of information security management systems, one of them is a measure of the effectiveness of the performance of ISMS controls. (Aldya,2019)

Usually, the effectiveness of the information system is measured by True-Positive (TP), True-negative (TN), False-Positive (FP), False-Negative (FN), and the below figure shows the example showing actual and predicted positive and negative classes in the test set.



	Predicted class POSITIVE (spam ✉)	Predicted class NEGATIVE (normal ✉)
Actual class POSITIVE (spam ✉)	TRUE POSITIVE (TP) ✉ ✉ 320	FALSE NEGATIVE (FN) ✉ ✉ 43
Actual class NEGATIVE (normal ✉)	FALSE POSITIVE (FP) ✉ ✉ 20	TRUE NEGATIVE (TN) ✉ ✉ 538

Fig 2: example table figure (source: Maarit, 2019)

TASK 2

Critically analysing few Frameworks of Information governance (IG) and possible framework recommendations for Air MSky.

To benefit from IG, choosing an appropriate framework is essential. A framework can help implement best practices policies and procedures that allow Air Msky or any organisation to maintain their programme year after year.

Frameworks	Description	Advantages	Disadvantages
COBIT	COBIT framework is an IT executive's system designed by the ISACA to assist organisations with creating	COBIT is flexible and gives a controlled environment that is receptive to business needs and serves the	Complex ideas and arrangement and Lack of execution guidance and also few specialists imagine that probably

	techniques around data from the board and administration.	executives and audit terms regarding their control liabilities.	the most significant disadvantage with COBIT is that it requires a lot of information to comprehend COBIT system before it very well may be applied as a device to support IT administration or evaluate the IT organisation's performance. (Zhang, Fever, 2013)
NIST	NIST framework is a robust implementation for overseeing and developing cyber security programs. It is a bunch of rules and finest procedures to aid associations with building and fortifying their cyber security position. The framework advances many suggestions and principles that empower organisations to distinguish and recognise cyber-attacks and give rules on the most proficient method to react, forestall, and recuperate from cyber incidents.	NIST is by a wide margin the most flexible structure given its risk-based, results-driven methodology. Numerous industries effectively embrace them.	NIST framework is that NIST cannot deal with shared liability. Nowadays, most organisations use the cloud with SaaS or PaaS offers by third-party companies. Consenting to NIST will mean, in this context, that you are on top of all the parts of your systems you manage yourself – but unfortunately, you will have almost zero commands over those parts that are managed remotely. (SamBocetta,2021)
GDPR	GDPR has been in since May 2018, replacing existing data protection laws in all EU countries. GDPR affects all organisations in the EU and every company outside the EU that desires to do business within the EU. The purpose of GDPR is "…the protection of natural persons concerning the handling of individual	Conforming to the GDPR assists organisations with reducing expenses by provoking to resign any information software and inheritance applications which is not relevant to the business. Following the GDPR's order to stay up to date decreases the storage expense by consolidating information present in	One of the most significant disadvantages of GDPR is the amount it costs for companies to get their information affairs in order and compliance. It took time and money.

	information and the free development of such data”. (Brodin,2019)	silos or stored in inconsistent formats.	

ISO/IEC 27001 framework recommendation for Air Msky

In our scenario, the Air Msky safety and security must be in the crucial role of significant importance and maintain a good security record and reputation. Concerning digitalisation and the reception of arising advancements that have expanded the danger of data and cybersecurity threats.

A robust framework Internationally recognised, ISO/IEC 27001, is needed for Air Msky, which helps ensure confidentiality, integrity, and availability of information, such as economic data, intellectual property, or sensitive customer data. It helps to identify risks and put appropriate security measures to manage them. So, ISO/IEC 27001 protects organisations and reputations, too.

Aligning ISO/IEC 27001 with AS EN 9100-series

Due to the ISO high-level structure, ISO/IEC 27001 aligns to the new AS EN 9100-series, integrating information security into Aerospace Quality Management System. Complementary management systems allow organizations to anticipate, adapt, and respond to the risks and opportunities created by a highly competitive, innovative industry like Air Msky, which provides organizations, large and small, with the resilience and agility needed to thrive globally market. (Bsi,2021)

Benefits of Implementing ISO 27001

ISO/IEC 27001 will help Air Msky across the organisations, vast and tiny, deal with a scope of data and network safety risks. More explicitly:

- Travel planners handle enormous volumes of traveller information and, in this manner, face the danger of cyberattacks.

- Data breaches involving passenger information, a compromised security surveillance system, customs and passport control, border services, homeland defence, and air traffic control pose risks to airports. When it comes to an understanding, such data flows and ensuring appropriate management, and ISO/IEC 27001 provides a best practice framework. (Bsi,2021)

- Airlines also face the threat of passenger data attacks on big data live streaming services, communications, and Wi-Fi. Assessing, prioritising, and reacting to the risk this pose is required by ISO/IEC 27001. (Bsi,2021)

With 114 different security controls in ISO/IEC 27001, there is a toolkit for minimizing organization's risk to a level that is acceptable.

Other ISO/IEC 27001 benefits include:

- ➢ Reputation and stakeholder confidence improves
- ➢ Better visibility of risk amongst interested parties
- ➢ Enhancing trust and credibility in the market to help you win more business
- ➢ Reduction of fines and prosecutions
- ➢ Further developed information security awareness among every significant party
- ➢ Reduced likelihood of staff-related information security breaches
- ➢ Increased organizational resilience
- ➢ cost reduction by minimizing threats

TASK 3

Risk Assessment and Activities:

Cyber security risk assessment has become a fundamental component of any data security program. Yet, as the innovation scene develops, ensuring an organization's information isn't vulnerable to a potential danger has become slightly more complicated. (Mark ,2020)

All in all, how would we get an extensive assessment of the Air Msky organization's weakness level? What's more, where do we begin? We should see a few responses to these questions.

This study's risk assessment activities will refer to the ISO 27005 standards, and the below fig.3 indicates the risk activities.

Fig. 3 indicates the risk assessment activities (Section III), aligned with the literature review (Section II) and objectives (Section I), and guided by the ISO 27005 standards in Fig.4. (Alwi and Ariffin, 2018)

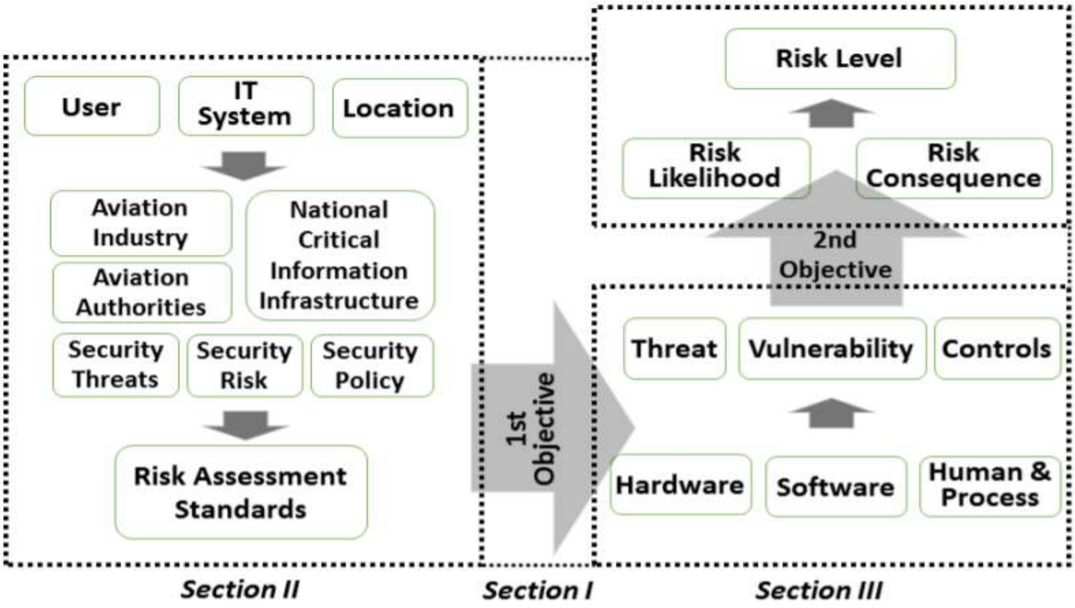


Fig 3. Risk assessment activities work process aligned with the objectives furthermore writing audit.

Source:(Alwi and Ariffin, 2018)

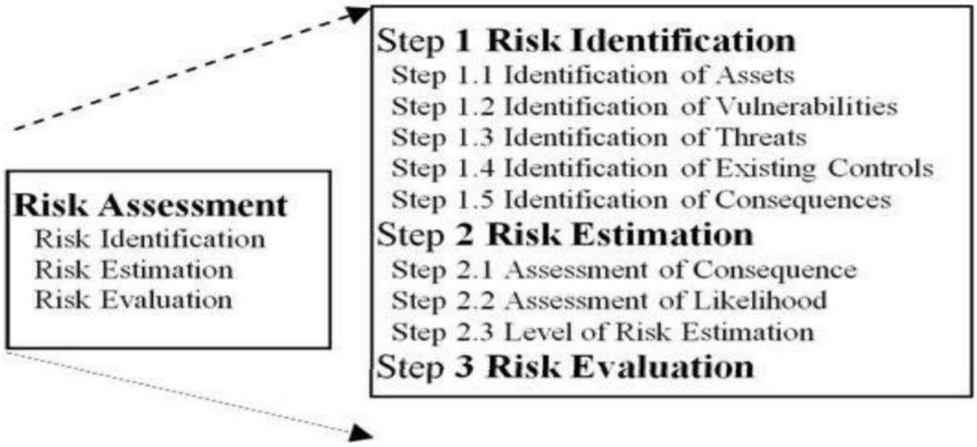

Risk Assessment
Risk Identification
Risk Estimation
Risk Evaluation
Step 1 Risk Identification
Step 1.1 Identification of Assets
Step 1.2 Identification of Vulnerabilities
Step 1.3 Identification of Threats
Step 1.4 Identification of Existing Controls
Step 1.5 Identification of Consequences
Step 2 Risk Estimation
Step 2.1 Assessment of Consequence
Step 2.2 Assessment of Likelihood
Step 2.3 Level of Risk Estimation
Step 3 Risk Evaluation

Fig 4: Risk Assessment guidelines by ISO 27005 standard. Source:(Alwi and Ariffin, 2018)

Risk Assessment (Identification, Estimation and Evaluation)

Asset identification:

find valuable assets across all the Air Msky that threats could harm in a way that results in a financial loss. A few examples for that:

- Servers
- Trade secrets
- Website
- Partner documents
- Customer credit card data
- Client contact information

Hardware

Physically, Air Msky infrastructure's configuration may expose risks due to system installation and design. It isn't easy to control the security of the system infrastructure if it is not centralised in the data centre. The information system needs to be satisfactorily prepared to ensure no unauthorised access to the physical system. Without clear strategies and methodology, the accessibility of physical infrastructure, frequent maintenance and monitoring will not be achieved. (Alwi and Ariffin, 2018)

Software

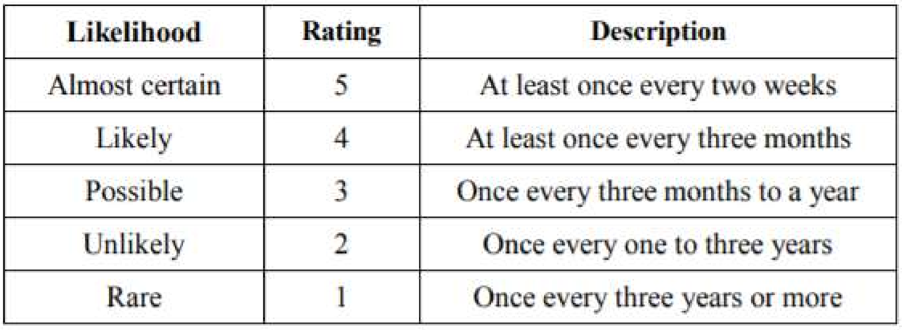
Software is also vulnerable to risk if there is no access control. For Air Msky, changes to the software are not recommended, such as deactivating a function to improve speed and performance. But if it is necessary for functional reasons, it needs to be carefully managed and documented. (Alwi and Ariffin, 2018)

Human and Process

This activity will look at risks caused by lack of expertise and tasks not organized in the Air MSky organization. Hence, the vulnerability factor under the human category is to be evaluated along with the process category. The process needs to be designated to ensure that the assigned staff is skilful and capable of operating the system. At the same time, dependency on only a few employees is also seen as a vulnerability and can be a threat to system availability. (Alwi and Ariffin, 2018)

Risk Likelihood.

It is the state of being probable or chance of a threat occurring event history and expected recurring risk surrounding Air Msky operation:



Likelihood	Rating	Description
Almost certain	5	At least once every two weeks
Likely	4	At least once every three months
Possible	3	Once every three months to a year
Unlikely	2	Once every one to three years
Rare	1	Once every three years or more

Likelihood ratings Source:(Alwi and Ariffin, 2018)

Qualitative analysis

The qualitative analysis utilises subjective assessment to examine an Air Msky value or prospects based on non-quantifiable information, such as management expertise, industry cycles, the strength of research and development, and work relations. (Tim,2021)

The qualitative analysis contrasts with quantitative analysis, which centres around numbers found in reports such as balance sheets. However, the two techniques will often use to analyse Air Msky operations and assess its potential as an investment opportunity. (Tim,2021)

Quantitative analysis

Quantitative analysis (QA), also known as statistical analysis, is a method that uses mathematical and statistical methods, measurement, and research to understand behaviour. Quantitative analysis uses for measuring, evaluating, and valuing financial instruments, as well as predictive modelling, such as when predicting changes in a country's gross domestic product (GDP). Quantitative analysis uses to evaluate a financial instrument and predict real-world events such as changes in GDP. (Will ,2020)

Risk rating scheme in revenue

HIGH	**MODERATE**	**LOW**
>5000-2500$	**>500-5000$**	**0-500$**

Cyber risk table for Air MSky (Netwrix ,2021)

Threat	Vulnerability	Asset and consequences	Risk	Solution
System failure - Overheating in server room **HIGH**	Air conditioning system is ten years old **HIGH**	Servers. All services (websites, email, etc.) will be inaccessible for at least 3 hours(netwrix, 2021) **HIGH**	(Approximate loss of 50,000$ per occurrence) (netwrix,2021) **HIGH**	Buy a new air conditioner.
Natural disaster- flooding **Moderate**	Server room is on the top floor. **LOW**	Servers. All services will be unavailable	**LOW**	No action needed
Malicious human (DDOS) attack **HIGH**	Firewall configured properly and has good DDOS mitigation. **LOW**	Website will be unavailable. HIGH	(Approximate loss of 5000$ per hour of downtime) (netwrix,2021) **Moderate**	Monitor firewall
Accidental file deletions by humans **HIGH**	Backups are taken regularly.IT auditing software is in place. **LOW**	Critical data could be lost from files. But almost certainly could be restored from backup **Moderate**	**LOW**	Permission changes continue monitoring, privileged users, and backups.