# INFORMATION SECURITY MANAGEMENT PROPOSAL

## ISO27001 Standard-Based Information Systems Security Program

## MoveSynch Technologies

### Steering Committee Members



| Name | Student ID |
|---|---|
| Sinduja Mullangi | 530621100 |
| Lakshmi Priya Kumar | 530661737 |
| Bo Fu | 540245590 |
| Matin Aliyev | 541011493 |
| Shimei Meng | 530378215 |
| Deyuan Huang | 530789570 |

# 1 Background

MoveSynch Technologies has created its own space by leveraging the opportunities that arise from the intersection of the health and technology industries. A primary contributor to its position in the market is its flagship product, PulsePro. PulsePro is a fitness tracker that helps users keep track of indicators and factors of good health and fitness such as step counts, sleep behavior, etc. At present the strategic initiatives in mind to fuel further growth are as follows:

a. Offering more features such as customized health plans tailored to individual health data for better insurance coverage through insurance company collaboration.
b. Creating online communities that foster connection, progress and a sense of belonging, through social media integration.
c. Integration of cutting edge technologies like Artificial Intelligence to provide improved features such as tailored fitness plans.
d. Streamlining organizational processes and functions through initiatives such as production relocation, cost effective supplier management and delivery logistics for an overall boost to efficiency.
e. Increasing promotional efforts to capitalize the European market.
f. Capacity building and restructuring at the organizational level to enhance innovation.

These initiatives reflect the current needs and requirements of MoveSynch Technology. Consequently, they define the scope of activities that need to be considered by the security program.

# 2 Objectives

MoveSynch Technologies recognizes the need to improve its security posture as a result of its drive towards success. This document proposes an ISO 27001 based information security program to assess and improve MoveSynch's security practices through the following objectives:

a. Safeguard MoveSynch technologies users, data, resources and processes from threats and vulnerabilities that may lead to negative consequences for confidentiality, integrity and availability and hinder the development and management of its planned initiatives.
b. Develop risk management processes to effectively identify, analyze, evaluate and treat risks through relevant controls to ensure business continuity.
c. Ensure the alignment of the program with the overall strategic and business objectives through an effective security governance structure under leadership support.
d. Achieve regulatory and contractual compliance wherever applicable. This includes compliance for handling sensitive health data according to GDPR and upholding contract obligations in cases of third party data handling, services and collaborations.
e. Establish a security aware culture within MoveSynch Technologies that is built around effective communication and documentation to facilitate continuous monitoring and improvement through lessons learnt.
f. Ensure the program activities are carried out such that it follows the estimated budget and schedule through continuous monitoring and evaluation of key performance indicators.

# 3 Key Issues and Concerns Identified for IS Security

MoveSynch Technologies as a start-up company currently uses a basic information security plan which is inadequate or insufficient as the company's growth is rapid and increases visibility in the global market.

**a.** ***Sensitive data protection or security concern:-*** MoveSynch technologies flagship product, PulsePro collects users sensitive health information including their existing medical conditions, heart rate, blood pressure, body temperature and GPS location which significantly increases the risks of unauthorized access, data leakage or data breaches. The company's basic information security practices introduce potential risks in protecting these sensitive information and they need to ensure in implementing robust information security practices. If the company fails to implement strong security measures in protecting user sensitive information might lead to reputational

damage, loss of customer trust, damage to the brand reputation and financial loss caused due to cyber incidents (Jennifer, 2021; Healey, 2022).

b. ***Cloud security risk management:-*** MoveSynch technologies stores users' sensitive health related information locally and then back-up those data to cloud for enhanced security and accessibility which would increase vulnerabilities in the cloud platform's security system. The company with lack of knowledge on managing the cloud platform would exploit vulnerabilities by cyber intruders which is a security concern. The cloud security system with poor cloud security management might allow malicious attackers to exploit the system leading to data breaches, unauthorized access and data theft due to misconfiguration and insecure interfaces. If the company fails to manage the cloud security would compromise user privacy, confidentiality and integrity of sensitive data stored. The company's major concern is to achieve legal and regulatory compliance in protecting user data securely in the cloud environment (Check Point, 2024; Proofpoint, 2023).

c. ***Risks related to third-party insurance companies:-*** MoveSynch technologies partners with insurance companies to improve the PulsePro's features to users providing personalized plans based on their tracked activities which raises the concerns about data sharing, security and privacy. The company should ensure that the user sensitive information is shared with the insurance companies in compliance with regulations for protecting user data. If the company fails to comply with these regulations could lead to legal penalties, fines, lawsuit-actions and reputational damage. They need to ensure that the data shared is accurate and updated to maintain data integrity, failing to achieve this will lead to liability and accountability issues. The company will introduce system vulnerabilities when collaborating which creates opportunities for attackers to exploit the company's system network, resulting in loss of data, ransomware attacks and operational disruptions. If the company fails to manage the risks such as data breaches, intellectual property theft, unauthorized access to user sensitive information, associated with the insurance company will lead to financial loss, loss of customer trust and brand reputation (Meyer, 2024; Metomic, 2022).

d. ***Risks associated with Social-Media Integration:-*** MoveSynch technologies integrates with Social-media to enhance its features enabling users to connect with each other, track their progress and participate in challenges to earn rewards which helps in fostering user engagement and brand loyalty. The company is responsible to ensure user data is secured and protected from exposure to cyberattacks such as data breach, identity theft, phishing, hacking and social engineering. They need to ensure strong security strategies or measures to protect user accounts and properly manage user preferences while processing their information legitimately. The company needs to ensure that they are legally compliant with regulatory standards and privacy legislations. If the company fails to implement these strategies or address these risks associated with it would lead to unauthorized access or misuse of user information. The company's poor social media management would lead to reputational damage and customer dissatisfaction (Virtina, 2023; Business Queensland, 2023).

e. ***AI related issues:-*** MoveSynch technologies launches AI-driven personal training features to provide customized work-out plans and real-time feedback to the users. The company needs to ensure that the data used or processed for the purpose of this feature is accurate and maintains integrity and confidentiality. If the data is inaccurate then it affects the result of the healthcare recommendation product which impacts on user experience and product reliability. The company needs to ensure strong protection measures to safeguard data manipulation or data poisoning of AI from the cyber intruders who can manipulate or poison the training dataset of AI model with malicious data which can harm users by producing inappropriate or malicious outcomes. If the company fails to implement these strategies to avoid malfunctions or security breaches would cause reputational damage, fines, and penalties which could also lead to data loss (Trend Micro, 2024; MalwareBytes, 2023).

f. ***Issues related to marketing and promotional campaigns:-*** In recent times, MoveSynch technologies flagship product, PulsePro has gained attraction from the European market by leading the business to expand its operation in that region. The company has appointed external

marketing and advertising agencies to launch marketing and promotional campaigns for their product to reach the targeted European customers. This introduces cross-border cybersecurity risks concerning data transfer, storage and processing. The company needs to ensure that it complies with the GDPR standard when expanding their business with the European Union. If the company fails to comply with this regulation, it might lead to legal consequences. The company needs to ensure that the external marketing and advertising agencies security practices align with their security standards to avoid security vulnerabilities leading to unauthorized access or exposure of user sensitive information (Indeed Editorial Team, 2024).

g. ***Supply chain management security risks:-*** MoveSynch Technologies integrates with the external third-party supplier to obtain high-quality materials for affordable price to enhance the production efficiency cost effectively. However, the involvement of third-party suppliers introduces third-party risks such as data security risks caused due to weak security practices in protecting sensitive information of users from cyber intruders or unauthorized access. This might also lead to the exposure of sensitive information causing threats such as ransomware attack, malicious injection, intellectual property theft, process disruption, data breaches and non-compliance with the regulatory standards to the company. There are data breach risks involved due to third-party suppliers affected from fraudulent activities and social engineering techniques (Kost, 2024).
h. ***Issues with in-house logistics and delivery department operation:-*** The establishment of in-house logistics and delivery department might pose significant risks such as ransomware attack and Denial-of-Service (DoS) attacks which could cause disruption in logistics operation and delay the courier delivery service. The department can be targeted by cyber intruders for phishing and malware attacks leading to unauthorized access. There could be threats involved due to malicious activities which might exploit user data related to their orders and payment details which exposes the company to vulnerabilities due to weak security protocols. It is the company's responsibility to ensure this department aligns with the company's policies and enforces strong security measures (KMT, 2023; Hassija et al., 2020).
i. ***Issues with talent acquisition and organizational restructuring:-*** MoveSynch technologies recruits new expertise for the research and development department which introduces potential risks related to access controls, role-based permissions, confidentiality concerns, data security concerns, insider threats, and lack of awareness on security management. The company when recruiting employees globally would encounter risk related to regulatory compliance and organizational culture. If the company does not align with its growth objective with the necessary support for its expansion operation with research and development department which involves organizational restructuring, then it leads to company's disruption due to poor management of organization structure. This could adversely impact morale, create confusion, reduce the focus, lead to communication issues and eventually affect productivity. The company experiences these risks if they fail to implement effective change management strategies and lack leadership involvement in their organization restructuring process (Foxall, 2023; L'Estrange, 2022; HRbrain, 2024).

The company needs to address these key issues identified to succeed in achieving their business objectives by implementing a standard-based information security management policy.

# 4 Why ISO 27001

The ISO/IEC 27001 standard is a standard published by the International Organization for Standardization for organizations across several industries to set up and prove their information security strength. It lays out a series of holistic and multidimensional guidelines, covering people, processes and technology, for developing an information security management system (ISO/IEC 27001:2022, n.d.). Given the current security posture and planned activities of MoveSynch Technologies, this standard provides a perfect fit for the following reasons (DataGuard, 2024; Drolet, 2024; Oro, 2024).

a. ISO27001 builds resilience against attacks from internal and external factors that could threaten the company such as confidentiality, integrity, availability and privacy breaches. MoveSynch requires heightened security, given the involvement of highly sensitive health data and third parties, that can be made possible through this standard.

b. MoveSynch Technology aims to achieve operational efficiency to save costs. ISO 27001 can help achieve this goal by streamlining and standardizing information flows that can ultimately reduce the risk of security incidents and its associated costs.
c. Improving and maintaining a good brand reputation is one of MoveSynch's primary goals. Through ISO 27001, it can show its users that MoveSynch prioritizes a security first approach that can help instill confidence in their products. Such a competitive advantage can also help in attracting top talent which can drive further innovation and growth.
d. ISO 27001's approach towards managing risks can help identify areas of concern and improvement from a security perspective to comply with regulations and avoid fines. This goes a long way in safeguarding the organization from the ever evolving threat landscape.

# 5 Key Components of the Security Program

## 5.1 Establishing Leadership and Commitment

According to ISO 27001, leadership and commitment refers to the ability of the top management of an organization to get involved with developing an information security management system. This involvement can take the form of setting up policies, defining organizational structure through roles and responsibilities and oversight of the functioning of the system.

MoveSynch Technologies can establish competent leadership in line with ISO27001 through the following steps (Fabiny, 2024; Agarwal, 2024; International Organization for Standardization, 2023):

a. Set an information security policy that is aligned with the company's planned initiatives, goals and context.
b. Set up key individuals who will be responsible for the activities outlined by the information security management system.
c. Integrate the information security management system processes with those of the company.
d. Set up and provide access to relevant resources to their respective departments to carry out tasks under the information security management system.
e. Set up communication channels organization-wide for effective communication to clearly and transparently communicate matters regarding the information security system.
f. Ensure the involvement and participation of different departments to create a culture that emphasizes security.
g. Ensure that the top management receives continuous reports regarding the status of the information security management system to verify that its intended outcomes are being achieved.

In this manner, effective leadership has the power to support overall business functioning while ensuring the company's commitment to security. Strong leadership commitment can support and ensure each of MoveSynch's planned initiatives are conducted smoothly through the seamless integration of security aspects into its business processes with adequate resource allocation. By including all the factors that are important to MoveSynch's activities, such as protection of user data, achieving regulatory compliance, inclusive of European market compliance, in the policies defined by executive leaders, MoveSynch Technologies can set up the groundwork for strong security mechanisms that support company goals. Leadership has the power to foster an attractive security culture that can help in the talent drive as well. Keeping in mind MoveSynch's ambition for growth on a larger scale, this leadership structure will ensure its security practices too are regularly reviewed and aligned with the company's trajectory.

## 5.2 Risk Assessment and Management

Risk assessment is the overall process of risk identification, analysis, evaluation, and management. It is the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects (International Organization for Standardization, 2018). They are a systematic process to identify, evaluate and reduce the potential risk for organizations and stakeholders. Due to the risk analysis and risk management being the central part in information security, we can focus on the

ISO31000 which is an international standard that provides guidelines for effective risk management. Using ISO 31000 can support achieving ISO 27001 compliance by providing a robust framework for risk management (Advisera, 2024).

According to the ISO 31000 and ISO27001, MoveSynch Technologies can follow the steps to build a well developed risk assessment and management system which contains overall risk management and continuous improvement (International Organization for Standardization, 2013; International Organization for Standardization, 2018).

a. ***Establish context:*** The company should first define the basic parameters for risk management and its process. These contain internal, external context, the need for risk management, the criteria and structure for risk.
b. ***Identity risks:*** According to the present situation of the company, it is necessary to identify what can happen, when and where it will happen and the reasons and methods that may happen.
c. ***Analysis risks:*** After confirming the specific situation of the risk, the company should quantify the degree of risk through mathematical methods and analyze its connection with existing control methods.
d. ***Evaluate risks:*** When getting the risk analysis, the company should make sure the level of risks by comparing it against criteria and then set the priorities.
e. ***Treat risks:*** In order to control the risks, the company should review existing guides for treating risks and make sure options for risk treatment and assessment of it.

The use of risk assessment systems has many benefits for the development of MoveSynch:

a. ***Provides a systematic way to make informed decisions:*** As a rapidly expanding company, MoveSynch Technologies will encounter more aspects and levels of risk issues, and the risk system can help more effectively select appropriate risk control solutions.
b. ***Economy and efficiency:*** By predicting and managing risks in advance and during project operation, it can effectively reduce the likelihood of surprises occurring which may greatly affect the overall planning and project progress of the company. This can help MoveSynch ensure controlled risks, reduce cost in risk resolution and take more investment in growing business.
c. ***Enhanced reputation:*** For MoveSynch Company to further expand its market, reputation is an important aspect. If there is information leakage or other breaches, it will greatly affect the company's customer trust and hinder further market expansion.

## 5.3 Operations Planning and Security

Operations planning and security relates to operational procedures and responsibilities, with a focus on planning, implementing and controlling processes to ensure the correct and safe use of information processing equipment and the implementation of risk management plans, while implementing and maintaining appropriate levels of information security and service delivery (Calder & Watkins, 2012; Disterer, 2013; ŢIGĂNOAIA, 2015)

MoveSynch Technologies is a fast-growing technology company that provides fitness tracker PulsePro and other products. Due to its strong market prospects, MoveSynch Technologies has recently planned to adjust and upgrade its products and services by creating online communities and introducing new AI-based features. These changes, even if smooth, are often disruptive to the business (Calder & Watkins, 2012). Proper Operations planning and controls can help MoveSynch Technologies reduce disruption to the company's business when changes to systems and applications occur, and when risks occur, to make MoveSynch Technologies products more stable and secure for users.

In order to implement measures to address risks and opportunities, MoveSynch Technologies shall plan, implement and control the required processes through the following steps in accordance with the established information security policy and the results of the information security risk assessment (Disterer, 2013; Viegas & Kuyucu, 2022):

a. Establish process guidelines for operating procedures according to the organization's information security policy, document them, and implement process control according to the process guidelines.
b. Documented information shall be provided to the extent and extent necessary to assure that the process has been carried out according to plan.
c. The organization shall approve, document and control changes to business processes, information processing facilities, operating systems and application software, and these changes shall be released under formal documentation control.
d. Organizations need to monitor resources and predict their usage to adjust their capacity to maintain desired performance.
e. The organization shall review the consequences of unintended changes and, if necessary, take action to mitigate negative effects.
f. The organization shall ensure that external (insurance companies and suppliers) processes, products and services provided in connection with the information security management system are controlled.
g. The organization shall, in accordance with established information security risk guidelines, perform information security risk assessments at planned intervals, or when significant changes are encountered, and maintain documents that record the results of information security risk assessments.

## 5.4 Organizational Roles, Responsibilities and Authorities

MoveSynch Technologies' recent development in the European market has given it a large user base, and in order to take advantage of its good prospects, MoveSynch Technologies plans to hire a large number of talents in the near future, cooperate with external insurance companies, and hired an external marketing and advertising firm to handle the marketing campaign for the European market. If these personnel (i.e., users, third-party companies, and employees of MoveSynch Technologies) do not know what rules they must follow and what behavior is expected of them, then the organization will be vulnerable (Kenyon, 2024).

Therefore, clearly defined roles, responsibilities and permissions are essential for the effective implementation and maintenance of information security management systems under ISO 27001. This ensures that everyone in the organization understands their role in protecting information security and contributes to overall security.

MoveSynch Technologies needs to follow these steps to define clear roles, responsibilities, and permissions (Kenyon, 2024; Viegas & Kuyucu, 2022):

a. Top management shall define and assign roles, responsibilities and authority for information security according to the needs of the organization, avoid conflicts between responsibilities and scope of responsibility, and ensure that roles, responsibilities and authority related to information security are properly allocated and communicated within the organization.
b. All employees of MoveSynch Technologies, third party companies such as insurance companies that work with MoveSynch Technologies, and the Movesynch Technologies user community should clarify their roles and responsibilities regarding information security, which should also be consistent with the organization's security policy.
c. Separation of responsibilities should be implemented to reduce the risk of unexpected changes to organizational systems.
d. All personnel shall implement information security in accordance with information security policies, subject-specific policies and procedures formulated by the organization.
e. Information shall be graded based on confidentiality, integrity, availability, and the organization's information security needs, and access to information and other related assets shall be provided, reviewed, adjusted, and removed in accordance with the organization's subject-specific policies and access control rules.

## 5.5 Regulatory Compliance

According to the ISO 27001, Regulatory compliance refers to an organization's adherence to laws, regulations, guidelines, and specifications relevant to its business processes. For data protection, MoveSynch should obey the Corresponding laws which include the General Data Protection Regulation (GDPR) and the Australian Privacy Act. Using these laws, the company should handle personal data to protect individuals' privacy and ensure data security (GDPR Advisor, 2024).

MoveSynch Technologies can follow the steps to build the Specify a complete process for data collection, storage, and sharing system (International Organization for Standardization, 2013; European Union, 2016).

a. ***Build consent management:*** the company should first clarify their purpose for collecting users data and Obtain user consent using accurate and clear language. Then it is also necessary to build a consent management system where users can independently manage their consent.
b. ***Build data review mechanism:*** The company should regularly inspect the using and storage for the data, it is necessary to make sure Data only be used in the claimed purpose (Data limitations) and timely deleted data that is no longer needed (storage limitation).
c. ***Build data breach Response Plan:*** When the data breaches happen, it is essential to inform the authority and users of the scope and degree of data leakage in time. And also give the users support to mitigate the risk.
d. ***Enhance employee training and awareness:*** Conduct regular training sessions for employees to ensure they understand their responsibilities under GDPR and the Australian Privacy Act. This helps in fostering a culture of data protection within the organization.
e. ***Enhance third-party management:*** Before using the services for third-party, such as data analysis, it is necessary to get the consent from the users. And also the company should ensure that third-party vendors and partners comply with data protection regulations. This can be achieved through data processing agreements and regular audits.

The use of Regulatory Compliance has many benefits for the development of MoveSynch:

a. ***Reducing the possibility of illegality and avoiding Penalties:*** Because MoveSynch will focus on European markets, the company will inevitably collect and use European data, in other words, it needs to comply with relevant GDPR laws. If there are no corresponding rules and regulations, one may face high fines.
b. ***Building trust and improving user satisfaction:*** User trust is crucial for the expansion of MoveSynch, and a rigorous privacy protection plan can demonstrate the company's professionalism, enhance user perception and satisfaction.
c. ***Enhancing data security:*** MoveSynch will use the supplier or other third-party companies, this may include the data sharing. Controlling and understanding policies can help reduce data breaches and other data issues during the process and help mitigate risks.

## 5.6 Human Resource Security

Human Resource security focuses on ensuring that employees are adequately screened, trained, and made aware of their responsibilities in information security, thereby reducing information security risks caused by human error, misuse of facilities, or malicious intent (Calder & Watkins, 2012).

MoveSynch Technologies plans to recruit professionals from both within and outside Australia. In order to accommodate the growth of personnel within the organization, and reduce the information security risks caused by the growth of personnel, MoveSynch Technologies should ensure human resource security through the following steps (Viegas & Kuyucu, 2022; Calder & Watkins, 2012):

a. The organization must implement appropriate processes to ensure its employees and contractors are appropriate for their roles before they are hired, while working with the organization, and upon termination.

b. The Organization shall ensure that employees and contractors understand the information security policy, their responsibilities and obligations, and the effects and consequences of non-compliance with information security management system requirements.
c. Identify the competencies required of the staff who will have an impact on information security and ensure that the staff assigned to the relevant work has the necessary competence and experience.
d. Ensure that all employees receive appropriate safety awareness training and other training, and conduct regular updates and communication.
e. The organization should appropriately document the above processes as evidence.

## 5.7 Communication Management

According to ISO 27001, Communication Management refers to the processes and protocols established to ensure effective communication regarding information security within an organization (International Organization for Standardization, 2013). These include internal and external communication which is for employees and for customers,third-parties.Well developed communication Management can timely and effectively keep abreast of the latest developments or updating to ensure the advancement of business (Sharron, 2023).

MoveSynch Technologies can follow the steps to build the standardized management methods for internal and external communication (International Organization for Standardization, 2013; StandardFusion, 2024).

For internal communication: -

**a.** ***Security awareness training:*** The company needs to establish corresponding courses and seminars to enhance employees' awareness of data security, such as password protection, identification of phishing emails, and so on.
**b.** ***Regular updates and audit:*** The company needs to inform employees of the results of system and system updates through email or other formal means, and regularly conduct data reviews and access action checks on employees to ensure that they have no improper operations.

For external communication: -

**a.** ***Customer notifications:*** The company needs to communicate with customers in terms of customer information processing. This includes the need to obtain user permission before collecting and using customer data, a system that allows users to independently manage their permissions, and an obligation to notify in case of any issues or leaks.
**b.** ***Third-Party communication:*** The company needs to ensure that third-party companies can guarantee the secure storage and legal use of information and needs to witness the qualifications of the third-party companies. We also need to consider potential issues and solutions in the process of sharing data

The use of Communication Management has many benefits for the development of MoveSynch:

**a.** ***Operational efficiency:*** Due to the increase in the size of MoveSynch the number of employees and the level of management departments will also greatly increase, which will increase the difficulty of communication. So clear communication channels help to quickly spread information and reduce the time needed to respond to security incidents.
**b.** ***Trust and transparency:*** The further development of MoveSynch requires the use of new suppliers, which requires clarifying the specific content of the company's data sharing with users to ensure transparency to users. Moreover, by selecting suitable suppliers, the company can also make customers trust its data protection capabilities more.

### 5.8 Documentation

The documentation is an important source of information required to record appropriate policies, procedures and risk management and maintenance plans needed to make the information security management system an efficient and structured approach for the company. The documentation prepared for MoveSynch company will cover the strategy that will be used to mitigate possible key issues such as proper handling of sensitive health data by cloud database providers and insurance companies during implementation of new possible initiatives. The documentation will be provided to supervise the security management system of MoveSynch in risk management and regulatory compliance aspects, as well as the implementation of the new functionalities that will require consistent procedures such as AI integrated health data analytics. The provided documentation should be updated periodically to ensure suitability with possible sensitive security operations and initiatives such as AI integrated personal training.

#### 5.8.1 Documentation Control

Documentation is an important data resource for standardization and monitoring of applied security systems and making continuous improvement in the system by reviewing and comparing records and audits. Given that MoveSynch will store customer data, privacy policies and risk plans, the company will ensure that the documentation is securely stored, available and can be used by authorized individuals. The proper distribution of information among insurance companies, research experts and other third parties will be ensured by the company. The access control to the documentation should also be strictly managed to ensure that all individuals can access to data they are authorized to, such as a cloud-based directory to access risk management and incident response data by employees. In case of loss prevention, the documentation will be secured with regular backups and a retention policy which suggests the possession of data for a defined period of interval and removal of unnecessary data when no longer necessary. By controlling the storage, protection, availability and adjustability of the documentation, the MoveSynch will ensure confidentiality and integrity of the applied security system in accordance with ISO 27001.

## 6 Cost Estimation

An essential component of any acquisition process, cost estimate aids in the assessment of resource needs at milestones and other crucial decision points by decision-makers (Cost Estimating and Assessment Guide - Best Practices for Developing and Managing Program Costs, 2020). To protect sensitive health data, maintain regulatory compliance, and foster business expansion, MoveSynch Technologies must invest in a robust Information Security Management System (ISMS) that complies with ISO/IEC 27001 standards. A cost analysis of the anticipated expenses related to creating and sustaining the security program may be found in this section. These expenses comprise staff, training, compliance, technology upgrades, external consulting, and both the initial setup and continuing operational costs. An outline of the main costs related to carrying out the program may be found below (Making a Business Case for Security: An Interagency Security Committee Best Practice, 2023).

| Cost Component | Estimated Cost (AUD) | Notes |
|---|---|---|
| 1. Consultation and Initial Audit | $50,000 | Hire professional external auditors to evaluate gaps and risks. |
| 2. Implementation (Tools/Tech) | $150,000 | Firewalls, encryption, SIEM, cloud security. |
| 3. Employee Training | $30,000 | Yearly security awareness and targeted training. |
| 4. Software Licensing | $100,000 | Endpoint security, DLP, and vulnerability scanning. |
| 5. Compliance Audits | $40,000/year | Ongoing audits for ISO 27001 and GDPR. |

| | | |
|---|---|---|
| 6. Personnel Costs | $250,000/year | IT auditors, security analysts, and CISOs. |
| 7. Insurance Premiums | $20,000/year | Covering for cyber liability. |
| **Total** | **$640,000** | **The annual cost may change depending on how it is actually implemented.** |

*Table 1: Cost Breakdown Overview for ISO/IEC 27001 Implementation*

1. Before implementing any security control measures, we need to hire external consultants or auditors to conduct preliminary audits, identify company vulnerabilities, gaps, and areas for improvement, in order to determine the current security situation of the company. For example, we can sign contracts with companies such as Deloitte or PwC to provide consulting services, and auditors will examine employee awareness, data storage protocols, cloud security, and compliance with pertinent laws like GDPR.
2. Once gaps and risks are discovered, technical security controls need to be implemented, including the following measures:
    a. Install advanced firewalls, such as Fortinet or Cisco ASA, to prevent unauthorized access.
    b. Use AES-256 encryption and other technologies to encrypt sensitive health data during transmission and at rest for local data storage and cloud backup.
    c. Implement SIEM systems such as Splunk or IBM QRadar to monitor security events in real-time and detect suspicious activities.
    d. Use services provided by cloud providers such as Amazon Web Services (AWS) or Microsoft Azure to enhance cloud security, which offers integrated security features such as encryption, identity management, and threat detection.
3. Employee training on secure communication, phishing awareness, best practices for data protection, and appropriate application of security controls installed within the company is crucial for maintaining security. Run an annual security awareness program provided by an external training provider of the SANS Institute, focusing on topics such as identifying phishing attacks and maintaining password security. For employees working in IT and customer support with high risks, it is necessary to ensure that they fully understand how to handle sensitive data and maintain security protocols.
4. To implement security policies and monitor potential vulnerabilities, MoveSynch needs to authorize various software tools (software licenses)
    a. Use Nessus vulnerability scanning program to continuously evaluate potential network vulnerabilities.
    b. Use Symantec DLP to prevent sensitive health information from leaving the organization's secure environment.
    c. Use McAfee or CrowdStrike to prevent malicious software, ransomware, and phishing attacks targeting employee devices.
5. In addition, regular audits of MoveSynch are required to ensure compliance with GDPR, the Australian Privacy Act, and any other regulatory standards related to the handling of personal health information.
    a. MoveSynch's compliance with data protection regulations and security frameworks (ISO 27001) was examined by an external compliance audit carried out by a third-party auditing firm.
    b. Penetration testing tests the system's defenses against simulated attacks.
6. Hire security experts responsible for monitoring, incident response, and ensuring compliance to establish or expand existing IT teams.
    a. Hire a Chief Security Officer to oversee the entire security plan.
    b. Hire security analysts to monitor SIEM alerts and provide real-time responses.
    c. Hire IT auditors to be responsible for internal audits.

7. As the business scale expands, MoveSynch's insurance vehicles also need to be adjusted, resulting in an increase in insurance costs.
    a. Cyber liability insurance protection against ransomware attacks, data breaches, and legal ramifications for breaking the GDPR or other standards.
    b. Paying the costs of legal defense while facing lawsuits or claims from persons impacted by data breaches.

# 7 Time Scheduling

This section outlines MoveSynch Technologies' phased approach to implementing ISMS, from initial risk assessment to continuous monitoring of security controls. Each stage is decomposed into manageable subtasks to ensure smooth deployment (Humphreys, 2016), and the following chart illustrates scheduling.

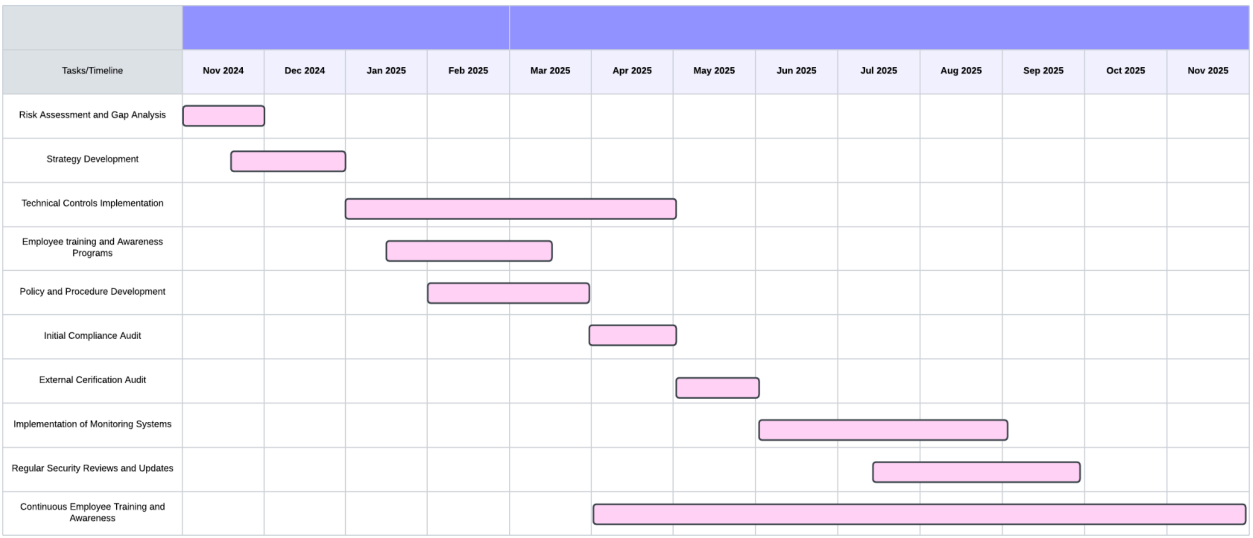


*Figure 1: Gantt chart of MoveSynch Technologies Scheduling*

***Phase 1: Initial planning and consultation (Month 1-2)***

MoveSynch Technologies will identify vulnerabilities in its present systems and evaluate potential hazards during this phase by conducting a thorough risk assessment and gap analysis. After that, a strategic action plan that outlines specific security targets in line with the organization's objectives will be created.

***Phase 2: Implementation of security controls (Month 3-6)***

In this phase, firewalls, encryption techniques, and Security Information and Event Management (SIEM) systems are examples of technical security controls that MoveSynch will put in place. Programs for employee training will be run concurrently to make sure staff members are knowledgeable about proper security measures. The business will also create thorough incident response and data protection practices.

***Phase 3: Compliance and auditing (Month 6-8)***

In this phase, MoveSynch is going to conduct an internal audit to make sure that GDPR regulations are being followed and to evaluate readiness for ISO/IEC 27001 compliance. After that, the formal ISO 27001 certification procedure will be finished by hiring an outside certification agency.

***Phase 4: Monitoring and continuous improvement (Month 9-12, ongoing)***

In the final phase, MoveSynch will set up real-time monitoring tools to identify and address security incidents. Additionally, the business will assess security on a regular basis and adjust its rules as needed. Staff will receive planned ongoing training to stay informed about new security procedures and risks.

# 8 Monitoring

As an improving start-up company, MoveSynch Technologies should opt to utilize a more structured and enhanced information security system. The forecasted improvements in system infrastructure and security bring crucial tasks such as continuous monitoring of the implemented information security management system to keep track of the performance and efficiency of the system and find new ways for possible improvements. Monitoring the efficiency of the security program will maintain alignment with key issues based on ISO 27001 standards as well as business deliverables. Monitoring practices aim to detect risks and vulnerabilities in each phase to secure continuous improvement. The monitoring practices cover regular internal audits and management reviews, and performance measurement to ensure consistent improvement.

a. ***Internal audit programme:*** MoveSynch is expected to establish an internal audit programme at defined intervals to analyze the alignment of the ISMS with the company's objectives and requirements. Monitoring should assess the effectiveness of policies and possible ways to maintain security measures. The internal audit programme should be based on feedback from previous audits and the importance of the process. MoveSynch should develop and control an audit programme based on frequency, responsibility, methods, and reporting. Auditors should ensure objectivity, and continuous audits should be conducted. Audit feedback should be documented and directed to management to provide evidence-based insights.
b. ***Management review:*** Higher administration must review the documentation and the ISMS over forecasted time periods to ensure sustainability, adequacy, and efficiency. Management feedback will consider the action status of past reviews, and relevant changes in internal/external issues and the expectations of shared parties.

## 8.1 Key Performance Indicators

a. ***Incident response time and frequency:*** As MoveSynch expands, improved incident response times are crucial in case of security breaches. The Incident Response Plan enables continuous monitoring, identification, eradication, and recovery of breaches. A security support center can help respond to incidents. The frequency of breaches can be monitored through automated detection systems. The technical team is expected to periodically review incidents with IT and management for further evaluation and timely response.
b. ***Risk management:*** A risk management team should create a risk management and treatment plan. As MoveSynch expands and introduces AI-related PulsePro functionalities, regular risk assessments should identify risks, which can then be managed using the risk treatment plan. Risk management should be continuous, given the sensitivity of customer health data.
c. ***Business process assurance:*** Aligning security practices with ISO 27001 standards will support the company's expansion into international markets. Key operational processes, including cloud usage and secure data storage, will be secured through the ISMS. Security processes will be integrated with overall business operations.
d. ***Continuous improvement:*** As MoveSynch reaches international markets, it must continuously improve the suitability and effectiveness of the security system. Nonconformities must be controlled and corrected. Nonconformities can be disregarded if unlikely to reoccur, but corrective actions must be documented to provide evidence of the results and nature of the issue.

# References


Advisera,(2024),ISO 27001 Risk Assessment, Treatment, & Management: The Complete Guide. https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/

Agarwal, H. (2024, March 6). ISO 27001 Leadership: All you need to know for implementation. UniSense Advisory. https://unisenseadvisory.com/iso-27001-leadership/

Business Queensland. (2023, June 29). *Social media for business*. Qld.gov.au; Queensland Government. https://www.business.qld.gov.au/running-business/marketing-sales/marketing/websites-social-media/social-media#risks-of-using-social-media

Calder, A., & Watkins, S. (2012). It governance : An international guide to data security and ISO27001/ISO27002. Kogan Page. IT Governance : an international guide to data security and ISO 27001/ISO 27002 - Calder, Alan - Watkins, Steve - IT Governance Publishing - Torrossa

Check Point. (2024). Top 15 Cloud Security Issues, Threats and Concerns. Check Point Software. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

Cost Estimating and Assessment Guide - Best Practices for Developing and Managing Program Costs. (2020). U.S. Department of Health and Human Services. https://www.gao.gov/pdf/product/705312

DataGuard. (2024, July 15). 12 Benefits of ISO 27001 compliance and certification - DataGuard. DataGuard. https://www.dataguard.co.uk/blog/benefits-of-iso-27001/

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(2). DOI: 10.4236/jis.2013.42011

Drolet, M. (2024). Council Post: ISO 27001 Certification: What It Is And Why You Need It. Forbes. [online] 12 Aug. Available at: https://www.forbes.com/councils/forbestechcouncil/2022/03/23/iso-27001-certification-what-it-is-and-why-you-need-it/.

European Union. (2016). General Data Protection Regulation (GDPR) (EU) 2016/679. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Fabiny, B. (2024, March 22). A focus on leadership, commitment, responsibility and information security policy in Clause 5. DQS. https://www.dqsglobal.com/en-au/learn/blog/iso-27001-clause-5-a-focus-on-leadership,-commitment,-responsibility-and-information-security-policy

Foxall, D. (2023, January 26). Five basic HR data security threats in 2018. Www.hrmsworld.com. https://www.hrmsworld.com/hr-data-security-threats.html

GDPR Advisor. (2024, September 17). *Integrating ISO 27001 into GDPR Compliance Strategies: A Detailed Guide*. https://www.gdpr-advisor.com/integrating-iso-27001-into-gdpr-compliance-strategies-a-detailed-guide/

Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures. IEEE Internet of Things Journal, 8(8). https://doi.org/10.1109/JIOT.2020.3025775

Healey, R. (2022, August 10). The Dangers of Sensitive Personal Data Exposure for Businesses. Formiti. https://formiti.com/the-dangers-of-sensitive-personal-data-exposure-for-businesses/

HRbrain. (2024, January 30). Human Resources Risk Assessment Best Practices. Hrbrain.ai. https://hrbrain.ai/blog/human-resources-risk-assessment-best-practices/

Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS Standard*. Artech house. https://books.google.com/books?hl=en&lr=&id=Yy6pCwAAQBAJ&oi=fnd&pg=PR6&dq=Humphreys,+E.+(2016).+Implementing+the+ISO/IEC+27001:+2013+ISMS+Standard.+Artech+house.&ots=vss3dnf8YQ&sig=Jpz4yvsvdT3Mz34ZKN7kA5zHHeg

Indeed Editorial Team. (2024, September 13). 10 Challenges in Marketing Challenges and How To Overcome Them. Indeed. https://www.indeed.com/career-advice/career-development/marketing-challenges

International Organization for Standardization. (2013). Information technology – Security techniques – Information security management systems – Requirements . https://www.iso.org/standard/54534.html

International Organization for Standardization. (2018). Risk management—Guidelines https://www.iso.org/standard/65694.html

International Organization for Standardization. (2023). ISO/IEC 27001:2023 Information security, cybersecurity and privacy protection — Information security management systems — Requirements . Retrieved from British Standards Online Via The University of Sydney Library.

ISO/IEC 27001:2022. (n.d.). ISO. https://www.iso.org/standard/27001

Jennifer. (2021, January 20). The risks of sensitive data exposure - OmniCyber Security. OmniCyber Security. https://www.omnicybersecurity.com/the-risks-of-sensitive-data-exposure/#:~:text=Attackers%20may%20steal%20or%20modify

Kenyon, B. (2024). *ISO 27001 Controls – A guide to implementing and auditing, Second edition*. Google Books. https://books.google.com.au/books?id=3R8UEQAAQBAJ&lpg=PA1&ots=3Ry87-udjl&dq=Organizational%20roles%2C%20responsibilities%20and%20authorities%20iso27001&lr&pg=PA27#v=onepage&q&f=false

KMT. (2023, May 10). Cyber Security and the Australian Transport & Logistics Sector. Kaine Mathrick Tech. https://kmtech.com.au/information-centre/cyber-security-and-the-australian-transport-logistics-sector/

Kost, E. (2024, September 16). The Biggest Security Risks in Your Supply Chain in 2024. Www.upguard.com. https://www.upguard.com/blog/biggest-supply-chain-security-risks

L'Estrange, J. (2022, November 8). The Risks of Organizational Restructuring. Red Clover. https://redcloverhr.com/risks-of-organizational-restructuring/

Making a Business Case for Security: An Interagency Security Committee Best Practice. (2023). https://www.cisa.gov/sites/default/files/2023-03/isc_making_a_business_case_for_security_2023_edition_508c.pdf

MalwareBytes. (2023). AI in Cyber Security: Risks of AI. Malwarebytes. https://www.malwarebytes.com/cybersecurity/basics/risks-of-ai-in-cyber-security

Metomic. (2022). Understanding Third Party Risk in Cyber Security. Metomic.io. https://www.metomic.io/resource-centre/third-party-risk-in-cyber-security#:~:text=Third%2Dparty%20risk%20in%20cyber

Meyer, M. (2024, January 5). 5 Common Data-Sharing Challenges & How to Overcome Them. Www.alation.com. https://www.alation.com/blog/data-sharing-challenges/

Oro. (2024, January 31). Eight key benefits of ISO 27001 compliance. Thoropass. https://thoropass.com/blog/compliance/benefits-of-iso-27001/

Proofpoint. (2023, April 28). What Is Cloud Security? - Issues & Threats. Proofpoint. https://www.proofpoint.com/au/threat-reference/cloud-security

Sharron, M. (2023, December 14). *ISO 27001 Requirement 7.4 – Communication*. ISMS.online. https://www.isms.online/iso-27001/7-4-communication/

StandardFusion. (2024). ISO 27001 – Understanding & Communicating with Stakeholders. https://www.standardfusion.com/blog/iso-27001-understanding-communicating-with-stakeholders

ŢIGĂNOAIA, B. (2015). Some Aspects Regarding the Information Security Management System within Organizations – Adopting the ISO/IEC 27001:2013 Standard. In *Studies in Informatics and Control* (Vols. 24–24, Issue 2). https://sic.ici.ro/documents/447/SIC_2015-2-Art8.pdf

Trend Micro. (2024, July 8). Top 10 AI Security Risks Every Business Should Know. Trend Micro. https://www.trendmicro.com/en_us/research/24/g/top-ai-security-risks.html#:~:text=AI%20and%20data%20risks

Viegas, V., & Kuyucu, O. (2022). IT security controls : a guide to corporate standards and frameworks. Apress. https://doi.org/10.1007/978-1-4842-7799-7

Virtina. (2023, May 12). Are You Risking Your Business with Social Media Integration? Virtina. https://virtina.com/risks-in-social-media-integration-to-your-business/

# Appendix

| Steering Committee member | Task Assigned<br>(each minimum 2 pages) |
|---|---|
| Sinduja Mullangi | ● Proposal structure<br>● Background<br>● Objectives<br>● Why ISO27001 Standard<br>● Establishing security governance and leadership<br>● Presentation |
| Lakshmi Priya Kumar | ● Identifying key issues and concerns for IS security<br>● Proposal formatting |
| Deyuan Huang | ● Risk assessment and management<br>● Regulatory compliance<br>● Communication management |
| Shimei Meng | ● Operation planning and security<br>● Organizational roles, responsibility and Authority<br>● Human Resource Security |
| Bo Fu | ● Cost Estimation<br>● Time Scheduling |
| Matin Aliyev | ● Documentation<br>● Monitoring |