A cover of a book with a city landscape

Description automatically generated

ISO 27001 Initial Assessment Report

for QUICKCOVER INSURANCE

Table of Contents

[EXECUTIVE SUMMARY 4](#_Toc141023588)

[Our Approach 5](#_Toc141023589)

[Key Participant Interviewed 5](#_Toc141023590)

[Maturity Level for each clause of ISO 27001 6](#_Toc141023591)

[Conclusions 7](#_Toc141023592)

[RoadMap 8](#_Toc141023593)

[Recommendations – ISMS activities 11](#_Toc141023594)

[Plan stage 11](#_Toc141023595)

[Do stage 15](#_Toc141023596)

[Check stage 16](#_Toc141023597)

[Act stage 17](#_Toc141023598)

[Recommendations – Annex A controls 18](#_Toc141023599)

[A.5 Information Security Policies 18](#_Toc141023600)

[A.6 Organization of Information Security 19](#_Toc141023601)

[A.7 Human resources security 21](#_Toc141023602)

[A.8 Asset management 23](#_Toc141023603)

[A.9 Access control 25](#_Toc141023604)

[A.10 Cryptography 29](#_Toc141023605)

[A.11 Physical and environmental security 30](#_Toc141023606)

[A.12 Operations security 33](#_Toc141023607)

[A.13 Communications security 38](#_Toc141023608)

[A.14 System acquisition, development and maintenance 40](#_Toc141023609)

[A.15 Supplier relationships 43](#_Toc141023610)

[A.16 Information security incident management 45](#_Toc141023611)

[A.17 Information security aspects of business continuity management 47](#_Toc141023612)

[A.18 Compliance 49](#_Toc141023613)

[SUMMARY 52](#_Toc141023614)

# EXECUTIVE SUMMARY

QuickCover Insurance has requested that an independent and trusted ISMS Auditor, conducts an assessment and analysis of the current state of the information security program of the organization and its compliance with ISO 27001:2013 standard. ISO 27001 (ISO 27001:2013) is an international standard for the implementation of a best practice Information Security Management System (ISMS). ISO 27001 accreditation requires an organization to bring information security under explicit management control.

The objective of the assessment was to document the current state of the ISMS and Annex A controls at its Head Office in London, United Kingdom, understand the state, and recommend actions needed to achieve the required state to prepare for ISO/IEC 27001 certification.

# Our Approach

Our approach is based on the interview and practical evaluation with the Owner/Manager, reviewing technical documentation and checking readiness to conduct ISO/IEC 27001 certification. All the findings are mapped on ISO/IEC 27001:2013 standard.

# Key Participant Interviewed

The first step of our assessment was the interview with the key participant to collect information and check on the practice in the organization. The respondent shared the information regarding information security in the organization, presented current controls of information security and answered questions from ISO 27001 checklists.

|  |  |
| --- | --- |
| **Position in the company** | **Respondent** |
| Owner/Manager | Jared Leto |

# Maturity Level for each clause of ISO 27001

To illustrate the conformity to ISO 27001, we have assigned a level of rank based upon the table below.

|  |  |
| --- | --- |
| **Observation Ranking (Conforms or Major and Minor non-conformity) (Conformity Rating)** | **Description** |
| **Major** | Significant improvement needed (major non-conformities and/or  significant number of minor non-conformities) |
| **Minor** | Minor to moderate improvement needed (minor non-conformities  and/or observations) |
| **Conforms** | Certification ready |
| **Observation** | Informational comment not impacting certification readiness |
| **Cannot be assessed** | The control cannot be assessed as it has not been neither designed or  implemented and it's applicability to QuickCover Insurance’s ISMS is not defined |

Addressing these shortfalls will require management commitment to establish, implement, maintain and improve a comprehensive ISMS.

# Conclusions

The line chart below provides a graphical summary of the assessment outcome. The chart describes the current level of ISO/IEC 27001:2013 Annex A control and the required maturity level, indicating significant gaps in the implementation of information security measures.

It is of utmost importance to prioritize the timely resolution of major non-conformities as they present substantial risks to the organization's information security. The presence of minor non-conformities highlights areas for improvement, indicating that some activities are currently reliant on trust and lack adequate security measures. To safeguard the business, it is imperative to thoroughly review every aspect and implement necessary measures to enhance protection and mitigate potential threats. By implementing and reviewing the identified level, QuickCover Insurance can significantly strengthen its overall security posture and reduce vulnerabilities.

*Figure 1. Graphical representation of each maturity level.*

# RoadMap

QuickCover Insurance needs to assign roles and responsibilities, to handle all actions related to the analysis of the non-conformity, execution of improvements and controls implementation to achieve the acceptable state for certification.

The table below shows ISO 27001:2013 controls ordered and prioritized by severity of the maturity levels. The table represents step by step guide to start executing improvements on minor non-conformity clauses and proceed with major non-conformity. It is highly recommended to follow the order, controls, which marked as Conforms, represent what is already in place and working well, minor non-conformities can be resolved by one-time activities, major non-conformities requires iterative, team-based approach, in order complete all activities, resolve issues effectively and in time.

The table can be treated as a project plan as presented in the table below, which represent required steps for successful transition and compliance.



|  |  |  |
| --- | --- | --- |
| **#** | С**ontrol** | **Maturity Level** |
|  | **Recommendations - Appendix A** | |
|  | A.7.1 Prior to employment | **Conforms** |
|  | A 11.1.1 & 2 Physical Security & Entry Controls | **Conforms** |
|  | A.11.2.9 Clear desk and clear screen policy | **Conforms** |
|  | A.8.1.1 Inventory of assets | **Conforms** |
| **1** |  | |
| 1.1 | A.6.1 Internal Organization | **Minor non-conformity** |
| 1.2. | A.12.3 Backup | **Minor non-conformity** |
| 1.3 | A.15.1 Information security in supplier relationships | **Minor non-conformity** |
| 1.4 | A.15.2 Supplier Service Delivery Management | **Minor non-conformity** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2** | |  | | | |
| 2.1 | | A.5.1 Management direction for information security | | **Major non-conformity** | |
| 2.2 | | A.6.2 Mobile devices and teleworking | | **Major non-conformity** | |
| 2.3 | | A.7.2 During employment | | **Major non-conformity** | |
| 2.4 | | A.8.1 Responsibility for assets | | **Major non-conformity** | |
| 2.5 | | A.8.2 Information Classification | | **Major non-conformity** | |
| s2.6 | | A.8.3 Media handling | | **Major non-conformity** | |
| 2.7 | | A.9.1 Business requirements for access control | | **Major non-conformity** | |
| 2.8 | | A.9.2 User access management | | **Major non-conformity** | |
| 2.9 | | A.9.3 User responsibilities | | **Major non-conformity** | |
| 2.10 | | A.9.4 System and application access control | | **Major non-conformity** | |
| 2.11 | | A.10.1 Cryptographic controls | | **Major non-conformity** | |
| 2.12 | | A.11.2 Equipment | | **Major non-conformity** | |
| 2.13 | | A.11.1.4 Protecting against external and environmental threats | | **Major non-conformity** | |
| 2.14 | | A.12.1 Operational procedures and responsibilities | | **Major non-conformity** | |
| 2.15 | | A.12.2 Protection from malware | | **Major non-conformity** | |
| 2.16 | | A.12.4 Logging and Monitoring | | **Major non-conformity** | |
| 2.18 | | A.12.5 Controls of operational software | | **Major non-conformity** | |
| 2.19 | | A.12.6 Technical vulnerability management | | **Major non-conformity** | |
| 2.20 | | A.13.1 Network security management | | **Major non-conformity** | |
| 2.21 | | A.13.2 Information transfer | | **Major non-conformity** | |
| 2.22 | | A.14.1 Security requirements of information systems | | **Major non-conformity** | |
| 2.23 | | A.14.2.7 Outsourced development | | **Major non-conformity** | |
| 2.24 | | A.16.1 Management of information security incidents and improvements | | **Major non-conformity** | |
| 2.25 | | A.17.1 Information security continuity | | **Major non-conformity** | |
| 2.26 | | A.18.2 Information security reviews | | **Major non-conformity** | |
| 2.27 | | A.18. Compliance | | **Major non-conformity** | |
|  | |  | |  | |
|  | | **Cannot be assessed** | | | |
|  | | A.12.7 Information systems audit considerations | | **Cannot be assessed** | |
|  | | A.15.2 Supplier service delivery management | | **Cannot be assessed** | |
|  | | **Recommendations – ISMS activities** | | |
| 3 | |  | | |
| 3.1 | | Scope Definition | | **Major non-conformity** |
| 3.2 | | Risk Assessment Approach and Execution | | **Major non-conformity** |
| 3.3 | | Treatment of Risks, including Statement of Applicability | | **Major non-conformity** |
| 3.4 | | Risk Treatment Plan | | **Major non-conformity** |
| 3.5 | | Monitoring, Review of the ISMS & Effectiveness of Controls | | **Major non-conformity** |
| 3.6 | | ISMS Improvement including Corrective & Preventive Actions | | **Major non-conformity** |

# Recommendations – ISMS activities

The tables on the subsequent pages include recommendations for improvements needed to achieve the level of maturity required for ISO 27001 certification.

The actions are divided into the Plan, Do, Check and Act phases of the QuickCover Insurance’s Information Security Management System (ISMS). The Plan-Do-Check-Act (PDCA) cycle is a continuous progress with each round the organization has the opportunity to (re-)define the scope of its Information Security Management System, (re-)define risks, (re-)select controls and adjust or create processes, policies and guidelines.

All activities listed within this section must be completed in advance of the initial certification audit.

Note, each stage of the PDCA cycle requires approach documents to be created (i.e. policy/ procedure documents). It is up to the discretion of management to determine if these documents should be created during the Plan stage or if they should be developed during the respective stages in which the documents will be used.

These recommendations represent typical activities needed to implement and operate an ISMS and to prepare for ISO 27001 certification. QuickCover Insurance management will need to ultimately decide what actions to undertake within their environment.

It is very important that QuickCover should take action in implementing controls for **Access Management, Network Security and Segregation of duties** to minimize the effect of attack while implementing other controls

## Plan stage

|  |  |
| --- | --- |
| **Scope Definition** | |
| **Short description** | The ISMS scope should be defined in terms of characteristics of the business,  the organization, its locations, assets and technologies. |
| **Observations** | * ISMS scope is not documented and approved by management. The scope contains the list of the areas, locations, assets, and technologies of the organization controlled by the ISMS. Exclusions from the scope are not documented and justified. |
| **Observation**  **Ranking** | * Major non-conformity |
| **Recommendations** | * Document ISMS scope including the list of the areas, locations, assets, and technologies of the organization. * Document all exclusions from ISMS scope (e.g., Insurance agents, offices security backup, vendor relationship, etc.), and justification for exclusion from scope. * Review and re-approve ISMS scope document with management annually or in cases if significant changes to the environment occur outside of the annual review cycle (e.g. regulatory changes, inclusion of new locations, etc.). |
| **Documents**  **reviewed** | Not in place |

|  |  |
| --- | --- |
| **Risk Assessment Approach and Execution** | |
| **Short description** | A Risk Assessment approach should be created for QuickCover Insurance. |
| **Observations** | * The organization has not developed and documented a comprehensive Risk Management Framework that describes all steps and relevant methods required to be carried out in terms of risk assessment process, including:   + Asset Identification   + Threat Identification   + Vulnerability Identification   + Control Analysis   + Likelihood Determination   + Impact Analysis   + Risk Determination   + Control Recommendations   + Results Documentation * The organization has not defined and documented the lists of assets that are included within ISMS scope. |

|  |  |
| --- | --- |
|  |  |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Create Risk Management Framework document contains risk levels matrix which is based on a 5-level scale (Very Low to Very High), and provides the instructions for risk level determination. * Adjust Risk Assessment Framework so that it includes the criteria for accepting risk and identifying the acceptable level of (e.g. at what level can risk automatically be accepted and under what circumstances). Approval should be obtained from high-level management for the decision to accept residual risks, and authorization obtained for the actual operation of the ISMS. * Review the documents containing the lists of assets and define a single comprehensive list of assets along with asset owners while considering above mentioned recommendation. |
| **Documents**  **reviewed** | This is On -going |

|  |  |
| --- | --- |
| **Treatment of Risks, including Statement of Applicability** | |
| **Short description** | Select the method for treating risks identified and obtain management  approval for the proposed residual risks. |
| **Observations** | * A Statement of Applicability (SOA) document is not available at QuickCover Insurance. * For the external certification Statement of Applicability is a key evidence of the steps taken between risk assessment and implementation of appropriate controls. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * The SOA document must be derived from the output of the risk assessment/ risk treatment plan and, if ISO 27001 compliance is to be achieved, must directly relate the selected controls back to the original risks they are intended to mitigate. * For each risk, the options for treatment must be evaluated (e.g. applying controls, accepting, avoiding or transferring risks) and actions are performed based on the selected option. Management approval is needed for each situation where risks are accepted. * A Statement of Applicability identifies whether each of the controls defined within Annex A of the ISO 27001 (or other relevant controls)   standard will be applied or not based on the Risk Treatment Plan. |

|  |  |
| --- | --- |
| **Documents reviewed** | Not in place |

## Do stage

|  |  |
| --- | --- |
| **Risk Treatment Plan** | |
| **Short description** | Formulate and implement a Risk Treatment Plan that outlines the management  action, resources, responsibilities and priorities needed to achieve the plan. |
| **Observations** | * The organization has not documented the requirements for Risk Treatment Plan creation and has not created Risk Treatment Plan template. |
| **Observation Ranking** | Major non-conformity |
| **Recommendations** | * Develop a comprehensive Risk Treatment Plan that would include:   + Appropriate management action. Management should agree with the Risk Treatment Plan and approve any risk acceptances.   + Resources. Management should assign resources (e.g. man-hours or budget) which can achieve the treatment of risk.   + Responsibilities for treatment. A responsible person/team should be identified who will manage the treatment process.   + Priorities for treatment. It should be identified which Risks are treated first; usually this will be the highest risks which take the least amount of effort to mitigate.   + Due date: Although this is not a required field, we recommend including it to set expectations regarding when actions will be achieved. * According to the document Risk Treatment Plan (in fact – Risk Assessment Report) should document identified risks and the decisions about how each of the identified risks should be handled. * Document detailed requirements for Risk Treatment (Action) Plan creation. * Annually review and re-approve the Risk Treatment document with management based on the outcomes of the Risk Assessment. |
| **Documents reviewed** | Not In Place |

## Check stage

|  |  |
| --- | --- |
| **Monitoring, Review of the ISMS & Effectiveness of Controls** | |
| **Short description** | The ISMS should be monitored to detect and act on errors and security incidents. Regular reviews on the effectiveness of the ISMS, the relevant  controls and the Risk Assessment should be performed |
| **Observations** | * The organization has not developed a document which describes the activities that should be taken at each stage of ISMS implementation, including “Check” stage. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Monitor and review procedures that are executed to detect and act on errors and security incidents. * Execute a security managers meeting in which all security related developments are discussed (e.g. errors and security incidents). Review the ISMS Policy and objectives, measure the effectiveness of controls and the Risk Assessment process. |
| **Documents reviewed** | Not in place |

## Act stage

|  |  |
| --- | --- |
| **ISMS Improvement including Corrective & Preventive Actions** | |
| **Short description** | After the Check phase (including several management reviews and the Internal  Audit), the ISMS should be improved through corrective & preventive actions. |
| **Observations** | * The organization has not developed a document which describes the activities that should be taken at each stage of ISMS implementation at QuickCover Insurance, including “Act” stage. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * QuickCover Insurance has to document Corrective and Preventive Action procedure which is aimed to ensure that problems, non-conformities, and improvements are dealt with in an efficient and effective manner, minimizing the chances of any recurrence. * Corrective and preventative actions should be documented in a consolidated repository or document after they are identified and should include:   + A description of the non-conformity (or potential non-conformity)   + A root-cause analysis of the non-conformity   + The actions needed to prevent recurrence   + The status of the action item - The actions identified should be implemented and the plan should be updated with the current status of the action   + The target date for implementation * The corrective and preventative actions and any improvements undertaken should be communicated to interested or impacted parties and management should confirm that these improvements/ actions achieve the intended objectives. * After the identification of the need for improvements or non-conformities through management reviews, Internal Audits, and other reviews, the corrective and preventive action plan should be updated and regularly reviewed by management. |
| **Documents**  **reviewed** | Not In Place |

# Recommendations – Annex A controls

The tables on the subsequent pages include recommendations for improvements to the Annex A controls. These recommendations were identified based on a review of the current state ISMS capabilities at QuickCover Insurance. The recommendations are grouped by processes and as a result, multiple Annex A controls may be addressed within each table.

These tables represent recommendations only and QuickCover Insurance management will need to ultimately decide what actions to undertake to add or improve the Annex A controls that support their ISMS.

## Information Security Policies

|  |  |
| --- | --- |
| **A.5.1 Management direction for information security** | |
| **Short description** | To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. |
| **ISO 27001 Control** | * + - 1. Policies for information security       2. Review of the policies for information security |
| **Observations** | * QuickCover Insurance does not have Security Policies. These are Standard Operating Procedures (SOP) covering different industry domains |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Divide information security policy into topic-specific policies, which further mandate the implementation of information security controls and are typically structured to address the needs of certain target groups within an organization or to cover certain topics. (e.g. mobile devices and teleworking, cryptographic controls, antivirus controls, management of technical vulnerabilities etc.) |
| **Documents reviewed** | Acceptable Use Policy and Privacy policy was seen |

## Organization of Information Security

|  |  |
| --- | --- |
| **A.6.1 Internal Organization** | |
| **Short description** | To establish a management framework to initiate and control the  implementation and operation of information security within the organization. |
| **ISO 27001 Control** | * + - 1. Information security roles and responsibilities       2. Segregation of duties       3. Contact with authorities       4. Contact with special interest groups       5. Information security in project management |
| **Observations** | * Manager/Owner is responsible for establishing, maintaining and enforcing information security policies within the Company. Security strategies and policies are approved by IT Officer. They are reviewed annually or if any incidents recorded pose any vulnerability which is not defined or mentioned in security policies. * There is no segregation of duty for operations * QuickCover Insurance has requested an auditor, as an independent and trusted partner, conducts an assessment and analysis of the current state of the information security level of the organization. * QuickCover Insurance has no procedure for its information security. |
| **Observation**  **Ranking** | Minor non-conformity |
| **Recommendations** | * Appoint an owner for each policy that will be drafted who then becomes responsible for its day-to-day implementation. |

|  |  |
| --- | --- |
| **Documents reviewed** | Not In place |

|  |  |
| --- | --- |
| **A.6.2 Mobile devices and teleworking** | |
| **Short description** | To ensure the security of teleworking and use of mobile devices. Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as “telecommuting”, “flexible  workplace”, “remote work” and “virtual work” environments. |
| **ISO 27001 Control** | * + - 1. Mobile device policy       2. Teleworking |
| **Observations** | * Staff uses company-owned mobile devices for remote working * QuickCover Insurance does not utilize any MDM solutions. * QuickCover Insurance does not have a policy that defines the conditions and restrictions for using teleworking. Most of employees work on corporate laptops, there are also employees who work on their own laptops. The organization leaves the staff to protect their asset based on maturity . * QuickCover Insurance does not have a policy that defines whether antivirus and automatic software update are turned on each laptop: corporate or private. * There is no BYOD documented policy. * Employees are allowed to work remotely connecting to any network, no VPN in place. * There is no policy or procedure describing usage of public Wi-Fi   networks. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Implement document named Teleworking policy to ensure that teleworking is undertaken safely from an information security perspective Describe teleworking/remote activities, acceptable use of information processing facilities, guidelines in the use of public Wi-Fi networks and prohibited activities. |
| **Documents reviewed** | No document in place |

## Human resources security

|  |  |
| --- | --- |
| **A.7.1 Prior to employment** | |
| **Short description** | To ensure that employees and contractors understand their responsibilities and  are suitable for the roles for which they are considered. |
| **ISO 27001 Control** | * + - 1. Screening       2. Terms and conditions of employment |
| **Observations** | * QuickCover Insurance uses policy with background check procedures. * Basic prescreening is done before employment - check social networks, such as LinkedIn, Facebook etc. if these links are submitted in CV * Contracts include confidentiality clauses are signed between staff and contractors. Also, NDAs are signed for Employees prior joining the company. * Terms and conditions of employment are documented in Employee Handbook, Onboarding Procedure from third party vendor |
| **Observation**  **Ranking** | Conforms |
| **Recommendations** | While using a third party for screening, it is important that QuickCover Insurance has an independent onboarding policy |
| **Documents reviewed** | Background Check Policy and Procedure Employee Handbook 2022  NDA - QuickCover Insurance |

|  |  |
| --- | --- |
| **A.7.2 During employment** | |
| **Short description** | To ensure that employees and contractors are aware of and fulfil their information security responsibilities. |
| **ISO 27001 Control** | * + - 1. Management responsibilities       2. Information security awareness, education and training       3. Disciplinary process |
| **Observations** | * QuickCover Insurance annually conducts trainings for its employees, on Information Security training, Security Awareness with a 15 minutes video. * QuickCover Insurance is does not carry out audits to follow the safe working process of employees. |

|  |  |
| --- | --- |
|  | * QuickCover Insurance does not have document procedures describing the disciplinary process in case of violation neither conditions of NDA nor IT security practices overall. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Implement document named Security Awareness policy that defines scope, procedures, topics, roles and responsibilities in terms of Awareness program. * Document and implement disciplinary process that are designed to provide a structured corrective action process to improve and prevent a recurrence of undesirable employee behavior and performance issues. |
| **Documents reviewed** | Not in Place |

## Asset management

|  |  |
| --- | --- |
| **A.8.1 Responsibility for assets** | |
| **Short description** | To identify organizational assets and define appropriate protection  responsibilities. |
| **ISO 27001 Control** | * + - 1. Inventory of assets       2. Ownership of assets       3. Acceptable use of assets       4. Return of assets |
| **Observations** | * QuickCover Insurance keeps an inventory of devices, books, which are issued to an employee. * Inventory of all assets associated with information and information processing facilities is carried out in form of Excel table without a detailed description of an asset and link to the owner. The table is updated manually by the Manager/ Owner once a year. * There is policy on acceptable use but needs to be reviewed * The employee resignation policy lacks procedure that would describe return the organization’s assets on termination of employment, namely corporate laptop and smartphone. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Document and implement a formal policy which establishes assets inventory and methods of inventory whether it is conducted manually or with help of automatic tools. For each asset organization must document sufficient information to identify the asset, its physical (or logical) location, information security classification. * Document and implement procedures acceptable use of applications, hardware, information and other information technology resources and systems. * Define the asset owners * Define proper termination procedure , revising the three- months of email access |
| **Documents reviewed** | Not in place |

|  |  |
| --- | --- |
| **A.8.2 Information Classification** | |
| **Short description** | To ensure that information receives an appropriate level of protection in  accordance with its importance to the organization. |
| **ISO 27001 Control** | * + - 1. Classification of information       2. Labelling of information       3. Handling of assets |
| **Observations** | * The process of information sharing is guided by “Need to know” basis. Document Control procedures, namely Paper Documentation chapter describes what paper documents should be considered as confidential. QuickCover Insurance doesn’t have policy covering classification of customer information. * Document Control procedures, namely Document Design chapter covers labelling of information. * QuickCover Insurance does not have any procedures or policies related to handling of assets for each information classification. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Add procedures describing classification of customer information which aims to ensure that information is handled according to the risk or impact to ensure the confidentiality, integrity and availability of data. |
| **Documents reviewed** | Not In Place |

|  |  |
| --- | --- |
| **A.8.3 Media handling** | |
| **Short description** | To prevent unauthorized disclosure, modification, removal or destruction of  information stored on media. |
| **ISO 27001 Control** | * + - 1. Management of removable media       2. Disposal of media       3. Physical media transfer |
| **Observations** | * QuickCover Insurance does not have procedures or policies regulating removable drives like USB or external hard drives. * QuickCover Insurance does not have procedures describing how are media disposed-of. If there is a special request from a customer, the media drive will be destroyed permanently. |

|  |  |
| --- | --- |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Create Removable Media Policy to minimize the risk of loss or exposure of sensitive information maintained by QuickCover Insurance and to reduce the risk of acquiring malware infections on computers operated by QuickCover Insurance. Document and implement procedures that would prohibit or allow acceptable usage of USB flash memory or external hard drives, define roles and responsibilities. |
| **Documents reviewed** | Not in place |

## Access control

|  |  |
| --- | --- |
| **A.9.1 Business requirements for access control** | |
| **Short description** | To limit access to information and information processing facilities. |
| **ISO 27001 Control** | * + - 1. Access control policy       2. Access to networks and network services |
| **Observations** | * No Access control policy and procedures described within Logical and Physical Security. * QuickCover Insurance has no policy which describe access to networks and network services (VPN, Wi-Fi). |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Have a Access control procedures in a separate policy. * Define who may access the services such as third party vendor and clients and describe the logical access conditions to those services. |
| **Documents reviewed** | Not In Place |

|  |  |
| --- | --- |
| **A.9.2 User access management** | |
| **Short description** | To ensure authorized user access and to prevent unauthorized access to  systems and services. |
| **ISO 27001 Control** | * + - 1. User registration and de-registration       2. User access provisioning |

|  |  |
| --- | --- |
|  | * + - 1. Management of privileged access rights       2. Management of secret authentication information of users       3. Review of user access rights       4. Removal or adjustment of access rights |
| **Observations** | * User registration and de-registration described in Onboarding and Adaptation, Employee resignation procedures. * Several administrator privileges, such as installing new software, granted to Microsoft Active Directory users or groups to perform certain operations. * QuickCover Insurance does not have procedures regulating employees privileged access rights. * Manager is responsible for giving certain permissions on emergency/special occasion. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Instead of giving Active Directory users local admin rights, limit it to certain number of rights via creating new organizational unit (OU). Organizational Units allow you to delegate admin tasks to users/groups without having to make him/her an administrator. * Please refer to **A.9.3.1** control regarding Management of secret authentication information. * Add procedures which would describe removal or adjustment of access rights during changes of employment. |
| **Documents reviewed** | Not in place |

|  |  |
| --- | --- |
| **A.9.3 User responsibilities** | |
| **Short description** | Users should be required to follow the organization’s practices in the use of secret authentication information. |
| **ISO 27001 Control** | A.9.3.1 Use of secret authentication information |
| **Observations** | * There are no documented procedures requiring usage of password managers from all employees. |
| **Observation**  **Ranking** | Major non-conformity |

|  |  |
| --- | --- |
| **Recommendations** | * Document and implement policy that outlines the need for well thought out password protection(e.g. usage of password managers: KeePass, OnePassword) |
| **Documents reviewed** | Not in Place |

|  |  |
| --- | --- |
| **Password managers to install (as a recommendation**  **)** | * **KeePassX** - free, open source, cross platform password manager. Supports multifactor authentication to your passwords database. KeePass being open source means that a number of people have reviewed the code and found it to be secure. * **1Password** - commercial password manager. The main advantage is that you can install app on all your devices and sync your password database. **1Password Teams** allows you to share password between certain group of people. There are admin controls to view and manage permissions to each shared password. |

|  |  |
| --- | --- |
| **A.9.4 System and application access control** | |
| **Short description** | To prevent unauthorized access to systems and applications. |
| **ISO 27001 Control** | * + - 1. Information access restriction       2. Secure log-on procedures       3. Password management system       4. Use of privileged utility programs       5. Access control to program source code |
| **Observations** | * Access to information and application systems such as VPN are not in place. * All QuickCover Insurance employees does not have Multifactor authentication configured on corporate mail account, it is informal rule, no documented procedures describing usage of MFA. * QuickCover Insurance does not have procedures restricting the use of system utilities. Active Directory users have privileged rights (see **A.9.2**). |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Please refer to **A.9.2.3** control regarding Use of privileged utility programs. |

|  |  |
| --- | --- |
|  | * Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also. * Please refer to **A.9.3.1** control regarding Password management systems. |
| **Documents reviewed** | Not in place |

## Cryptography

|  |  |
| --- | --- |
| **A.10.1 Cryptographic controls** | |
| **Short description** | To ensure proper and effective use of cryptography to protect the  confidentiality, authenticity and/or integrity of information. |
| **ISO 27001 Control** | * + - 1. Policy on the use of cryptographic controls       2. Key management |
| **Observations** | * There is no documented policy on the use of cryptographic controls. Consequently neither documented framework nor related controls were established. * There are no procedures that would define rules of Full Disk Encryption usage. * Key management process is not regulated within the organization. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Develop and implement cryptographic controls policy to establish requirements and procedures for the use of encryption techniques to protect sensitive data. Assign roles and responsibilities, e.g. who is responsible for:   1. the implementation of the policy;   2. the key management, including key generation. * Develop and implement policy or procedures needed to create, manage, distribute, use, store, and revoke cryptographic keys and digital certificates(e.g. public key infrastructure (PKI)) |
| **Documents reviewed** | Not in place |

## Physical and environmental security

|  |  |
| --- | --- |
| **A.11.1 Secure areas** | |
| **Short description** | To prevent unauthorized physical access, damage and interference to the  organization’s information and information processing facilities. |
| **ISO 27001 Control** | * + - 1. Physical security perimeter       2. Physical entry controls       3. Securing offices, rooms and facilities       4. Protecting against external and environmental threats       5. Working in secure areas       6. Delivery and loading areas |
| **Observations** | * There are surveillance CCTV cameras installed at entrances and exits. * Physical access control is not implemented. A physical log book is not maintained by the secretary. There is no electronic logging of each employee. * Paper documents are stored in-house in key and lock room. There is a defined group of people who have access to this room. * Central alert system is not configured. Informal procedures for alert of disaster is not present. * There is a guard on duty at the main entrance. The guard is responsible for alerting in case of emergency situation or natural disaster. * No documentation in place   . |
| **Observation**  **Ranking** | Minor non-conformity |
| **Recommendations** | * Install an electronic logging of each employee to ensure that only authorized personnel are allowed access to certain organization premises. * There should be a central alert system and procedures for disaster, in case of tornado * Create a policy to address the physical and environmental security |
| **Documents reviewed** | Not In Place |

|  |  |
| --- | --- |
| **A.11.2 Equipment** | |
| **Short description** | To prevent loss, damage, theft or compromise of assets and interruption to the  organization’s operations. |
| **ISO 27001 Control** | * + - 1. Equipment siting and protection       2. Supporting utilities       3. Cabling security |

|  |  |
| --- | --- |
|  | * + - 1. Equipment maintenance       2. Removal of assets       3. Security of equipment and assets off-premises       4. Secure disposal or reuse of equipment       5. Unattended user equipment       6. Clear desk and clear screen policy |
| **Observations** | * Equipment is sited in the protected areas which are equipped with:   + air conditioning system   + video surveillance system   + mechanical lock * Equipment is protected from power failures by UPS. * The organization purchases services of local laptop repair company. There are no documented procedures of equipment maintenance outside the organization's premise. Consequently neither documented framework nor related controls were established. * The organization does not perform verification of equipment prior to disposal in order to ensure that any sensitive data and licensed software has been removed or securely overwritten. * Managers practice informal verbal notification about screen locking, no related documented procedures were established. |
| **Observation**  **Ranking** | **`**Major non-conformity |
| **Recommendations** | * Create and document procedures defining correct equipment maintenance outside the organization's premise. Confidential information should be cleared from the equipment or full disk encryption(FDE) must be enabled . * Establish, document and implement Clear Desk Policy to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. * Document secure disposal procedures to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use by the vendor. Confidential information can be compromised through careless disposal or re-use of equipment. |
| **Documents reviewed** | Not in Place |

## Operations security

|  |  |
| --- | --- |
| **A.12.1 Operational procedures and responsibilities** | |
| **Short description** | To ensure correct and secure operations of information processing facilities. |
| **ISO 27001 Control** | * + - 1. Documented operating procedures       2. Change management       3. Capacity management       4. Separation of development, testing and operational environments |
| **Observations** | * The organization has defined requirements for documenting of operating procedures within organization. Some of operational procedures are documented selectively. * Change management process within the organization is regulated by Change Management SOP. The following key areas are covered by the policy:   + Software Change Control   + Document Change Control   + Contractual Change Control * Capacity management is represented for current state, there is an Excel table with all hardware models, also each new asset get predefined documented pack of hardware. * There is no policy of capacity projections which describes purchase plan for the next year.(Purchase plan for laptops, mobile devices, printers, other hardware) |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Create and document capacity projections which describes purchase plan for the next year. * Create and document comprehensive description of separation of development, testing and operational environments. |
| **Documents reviewed** | Not in place |

|  |  |
| --- | --- |
| **A.12.2 Protection from malware** | |
| **Short description** | To ensure that information and information processing facilities are protected  against malware. |
| **ISO 27001 Control** | A.12.2.1 Controls against malware |
| **Observations** | * The organization uses a third party vendor for the adopted of Anti-virus procedures which regulates protection against malicious code execution. It states that all QuickCover Insurance computers should have standard and supported anti-virus software. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Establishing a formal policy describing protection against malware. * Install and regular update malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the scan carried out should include:   1. scan any files received over networks or via any form of storage medium, for malware before use;   2. scan electronic mail attachments and downloads for malware before use; this scan should be carried out at different places, e.g. at electronic mail servers, desktop computers and when entering the network of the organization;   3. scan web pages for malware; |
| **Documents reviewed** | Not In Place |

|  |  |
| --- | --- |
| **A.12.3 Backup** | |
| **Short description** | To protect against loss of data |
| **ISO 27001 Control** | A.12.3.1 Information backup |
| **Observations** | * QuickCover Insurances uses mail services cloud services for information backup. * The surveillance backups for just 7 days before rolling over with no regular monitoring. * Back-up process is not regulated by a formal policy which describes requirements to backup/restore procedures (retention time, backup frequency, backup method) according to classified types of information.. * The organization has not defined requirements for regular execution of backup recoverability testing procedures as well as instructions for   their execution. |
| **Observation**  **Ranking** | Minor non-conformity |
| **Recommendations** | * Implement and document procedures describing regular testing of backup media to ensure that they can be relied upon for emergency use when necessary; this should be combined with a test of the restoration procedures and checked against the restoration time required. |
| **Documents reviewed** | Not In place |

|  |  |
| --- | --- |
| **A.12.4 Logging and monitoring** | |
| **Short description** | To record events and generate evidence. |

|  |  |
| --- | --- |
| **ISO 27001 Control** | * + - 1. Event logging       2. Protection of log information       3. Administrator and operator logs       4. Clock synchronization |
| **Observations** | * There is no formal policy to regulates types of logs which should be maintained and monitored within the organization, formal requirement to specific events which should be contained in these logs, logs retention periods, responsibilities of key process participants are not defined. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Develop, document, implement, and maintain effective log management policy/procedures throughout the company. |
| **Documents reviewed** | Not in place |

|  |  |
| --- | --- |
| **A.12.5 Control of operational software** | |
| **Short description** | To ensure the integrity of operational systems. |
| **ISO 27001 Control** | A.12.5.1 Installation of software on operational systems |
| **Observations** | * Employees installs software which is not related directly to work activities. * There is no documented procedures that would require users of workstations install software only from approved "White software list". * Installation of software on local operating systems is not properly controlled within organization. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Develop and implement procedures/controls for approving/restricting software installation on operating systems for user workstation. To restrict users possibility to install software on operating systems implement preventive technical controls, or detective procedures of checking software which is already installed. |

|  |  |
| --- | --- |
| **Documents reviewed** | Not in place |

|  |  |
| --- | --- |
| **A.12.6 Technical vulnerability management** | |
| **Short description** | To prevent exploitation of technical vulnerabilities. |
| **ISO 27001 Control** | * + - 1. Management of technical vulnerabilities       2. Restrictions on software installation |
| **Observations** | * The organization has not implemented policy which defines roles, responsibilities, timelines and procedures within vulnerability management process. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Create, document and implement Vulnerability Management Policy to establish procedures for identifying and promptly remediating vulnerabilities to minimize security breaches associated with unpatched vulnerabilities. Establish and document guidelines for software installation which make users aware of what QuickCover Insurance deems as acceptable and unacceptable software that is installed (e.g. whitelists) |
| **Documents reviewed** | Not In Place |

**Nessus Professional** - a vulnerability assessment solution with the lowest false positive rate.

Main advantages:

* Ability to create and run custom scan.
* Nessus is partly proprietary - ability to write and add your own rules.
* Ability to import scan report to .csv or .pdf files.
* Intuitive and user-friendly interface, so you can install and start to scan your corporate perimeter immediately.

**Vulnerability management tools to install (as a recommendation )**

|  |  |
| --- | --- |
| **A.12.7 Information systems audit considerations** | |
| **Short description** | To minimize the impact of audit activities on operational systems. |
| **ISO 27001 Control** | A.12.7.1 Information systems audit controls |
| **Observations** | * Based on the results of Assessment, the organization did not identify any business needs of Information systems audit. Consequently neither documented framework nor related controls were established. |
| **Observation Ranking** | Cannot be assessed |
| **Recommendations** | N/a |
| **Documents reviewed** | N/a |

## Communications security

|  |  |
| --- | --- |
| **A.13.1 Network security management** | |
| **Short description** | To ensure the protection of information in networks and its supporting  information processing facilities |
| **ISO 27001 Control** | * + - 1. Network controls       2. Security of network services       3. Segregation in networks |
| **Observations** | * A network segmentation is not implemented. |
| **Observation**  **Ranking** | Major non-conformity |

|  |  |
| --- | --- |
| **Recommendations** | * Create formal documentation of network controls configuration. |
| **Documents reviewed** | Not In Place |

|  |  |
| --- | --- |
| **A.13.2 Information transfer** | |
| **Short description** | To maintain the security of information transferred within an organization and  with any external entity |
| **ISO 27001 Control** | * + - 1. Information transfer policies and procedures       2. Agreements on information transfer       3. Electronic messaging       4. Confidentiality or nondisclosure agreements |
| **Observations** | * There are no documented procedures that ensure that information is protected against unauthorized access, misuse or corruption during transfer. Neither documented framework nor related to information transfer controls were established. * There are no documented procedures describing transfer of secret authentication information, namely passwords. * QuickCover Insurance signs nondisclosure agreements with employees, clients and third parties. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Establish, document and implement policy that lays out the practical methods that need to be applied in undertaking a transfer of information. * Establish and document guidelines for electronic messaging usage which make users aware of what QuickCover Insurance deems as acceptable and unacceptable use of its messaging process. |
| **Documents reviewed** | Not In Place |

## System acquisition, development and maintenance

|  |  |
| --- | --- |
| **A.14.1 Security requirements of information systems** | |
| **Short description** | To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks. |
| **ISO 27001 Control** | * + - 1. Information security requirements analysis and specification       2. Securing application services on public networks       3. Protecting application services transactions |
| **Observations** | * Change management policy is not developed |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Create, document and define requirements for new information systems within Project Initiation policy or enhancements to existing information systems within Change Management policy. * Document usage of secure authentication methods for applications accessible via public networks e.g. using public key cryptography, digital signatures and multifactor authentication to reduce the risks |
| **Documents reviewed** | Not in place |

|  |  |
| --- | --- |
| **A.14.2 Security in development and support processes** | |
| **Short description** | To ensure that information security is designed and implemented within the  development lifecycle of information systems. |

|  |  |
| --- | --- |
| **ISO 27001 Control** | * + - 1. Secure development policy       2. System change control procedures       3. Technical review of applications after operating platform changes       4. Restrictions on changes to software packages       5. Secure system engineering principles       6. Secure development environment       7. Outsourced development       8. System security testing       9. System acceptance testing |
| **Observations** | * Based on the results of assessment, the organization did not identify any risks of service delivery within outsourced software development. Consequently neither documented framework nor related controls were established. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Document, apply and conduct penetration testing procedures on software releases. |

|  |  |
| --- | --- |
| **Documents reviewed** | N/A |

|  |  |
| --- | --- |
| **A.14.3 Test data** | |
| **Short description** | To ensure the protection of data used for testing |
| **ISO 27001 Control** | A.14.3.1 Protection of test data |
| **Observations** | * QuickCover Insurance doesn’t process data containing personally identifiable information or any other confidential information. * Therefore, based on the results of assessment, the organization did not identify any risks of service delivery within protection of test data. Consequently neither documented framework nor related controls were established. |
| **Observation**  **Ranking** | Cannot be assessed |
| **Recommendations** | N/A |
| **Documents reviewed** | N/A |

## Supplier relationships

|  |  |
| --- | --- |
| **A.15.1 Information security in supplier relationships** | |
| **Short description** | To ensure protection of the organization’s assets that is accessible by suppliers. |
| **ISO 27001 Control** | * + - 1. Information security policy for supplier relationships       2. Addressing security within supplier agreements       3. Information and communication technology supply chain |
| **Observations** | * All devices are purchased from authorized distributors. * QuickCover Insurance regularly gets certain number of license keys to activate Microsoft Windows operating systems. * The organization purchases services of local laptop repair company. |
| **Observation**  **Ranking** | Minor non-conformity |
| **Recommendations** | * Identify and document the types of suppliers, e.g. IT services, logistics utilities, financial services, destruction company, whom the organization will allow to access its information; * Identify information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization’s business needs and requirements. * Enable full disk encryption (FDE) on laptops which are transferred to laptop repair company. |
| **Documents reviewed** | N/A |

|  |  |
| --- | --- |
| **A.15.2 Supplier service delivery management** | |
| **Short description** | To maintain an agreed level of information security and service delivery in line  with supplier agreements. |
| **ISO 27001 Control** | * + - 1. Monitoring and review of supplier services       2. Managing changes to supplier services |
| **Observations** | * Based on the results of assessment, the organization did not identify any business need of monitoring, review, managing changes to supplier services. Consequently neither documented framework nor related controls were established. |
| **Observation**  **Ranking** | Cannot be assessed |

|  |  |
| --- | --- |
| **Recommendations** | N/A |
| **Documents reviewed** | N/A |

## Information security incident management

|  |  |
| --- | --- |
| **A.16.1 Management of information security incidents and improvements** | |
| **Short description** | To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and  weaknesses. |
| **ISO 27001 Control** | * + - 1. Responsibilities and procedures       2. Reporting information security events       3. Reporting information security weaknesses       4. Assessment of and decision on information security events       5. Response to information security incidents       6. Learning from information security incidents       7. Collection of evidence |
| **Observations** | * The organization has not adopted policy which regulates responsibilities and procedures in terms of information security incidents management process. * The organization has not formal policy which regulates reporting of information security incidents and weaknesses. * The organization has not documented procedures for learning from information security incidents and collecting evidence. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Establish, document, implement and maintain Incident Response Policy. Establish management responsibilities to ensure that the following procedures are developed and communicated adequately within the organization:   + procedures for incident response planning and preparation;   + procedures for monitoring, detecting, analyzing and reporting of information security events and incidents;   + procedures for handling of forensic evidence; * Prepare information security incident submission form to support the reporting action and to help the person reporting to remember all necessary actions in case of an information security event; * Make aware all employees and contractors of their responsibility to report information security events as quickly as possible. Situations to be considered for information security event reporting include:   + ineffective security control;   + breach of information integrity, confidentiality or availability expectations;   + human errors;   + non-compliances with policies or guidelines; |

|  |  |
| --- | --- |
|  | * breaches of physical security arrangements; * uncontrolled system changes; * malfunctions of software or hardware; * access violations. * Build an information security incident response team (ISIRT), so that the team assess and make decision on information security events. * Use anecdotes from actual information security incidents in user awareness training as examples of what could happen, how to respond to such incidents and how to avoid them in the future. |
| **Documents reviewed** | Not In Place |

## Information security aspects of business continuity management

|  |  |
| --- | --- |
| **A.17.1 Information security continuity** | |
| **Short description** | Information security continuity should be embedded in the organization’s  business continuity management systems. |
| **ISO 27001 Control** | * + - 1. Planning information security continuity       2. Implementing information security continuity       3. Verify, review and evaluate information security continuity |
| **Observations** | * QuickCover Insurance does not have Business continuity and Disaster Recovery policy. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Create and document the policy to contains Emergency Management Team, Data and Systems Recovery Timing, Disaster Recovery Activities. The organization should define and adopt two Scenarios for mitigation of emergency situation. * Regularly exercise and test business continuity plans to ensure that they are remain up to date and effective. * Integrate verification of information security continuity controls with the organization’s business continuity or disaster recovery tests. |
| **Documents reviewed** | Not In Place |

|  |  |
| --- | --- |
| **A.17.2 Redundancies** | |
| **Short description** | To ensure availability of information processing facilities. |
| **ISO 27001 Control** | A.17.2.1 Availability of information processing facilities |
| **Observations** | * Availability of information processing facilities is protected from power failures and other disruptions by UPS, redundant heating/ventilation and air-conditioning systems. |
| **Observation**  **Ranking** | Major non-conformity |

|  |  |
| --- | --- |
| **Recommendations** | * Test redundant information systems to ensure the failover from one component to another component works as intended. |
| **Documents reviewed** | Not In Place |

## Compliance

|  |  |
| --- | --- |
| **A.18.1 Compliance with legal and contractual requirements** | |
| **Short description** | To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. |
| **ISO 27001 Control** | * + - 1. Identification of applicable legislation and contractual requirements       2. Intellectual property rights       3. Protection of records       4. Privacy and protection of personally identifiable information       5. Regulation of cryptographic controls |
| **Observations** | * The organization makes employees sign personal data processing agreement with clients. * The organization did not outline all relevant legal requirement to ensure compliances |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Identify all legislation applicable to the organization in order to meet the requirements for business. If the organization conducts business in other countries, managers should consider compliance in all relevant countries. * Consider following guidelines to protect any material that may be considered intellectual property:   + publish an intellectual property rights compliance policy which defines the legal use of software and information products;   + acquire software only through known and reputable sources, to ensure that copyright is not violated;   + carry out reviews that only authorized software and licensed products are installed; * Take the following steps meet record safeguarding objectives:   + document guidelines on the retention, storage, handling and disposal of records and information;   + draw up a retention schedule identifying records and the period of time for which they should be retained; |

|  |  |
| --- | --- |
|  | - maintain an inventory of sources of key information   * Data protection policy should be communicated to all persons involved in the processing of personally identifiable information. |
| **Documents reviewed** | Not In Place |

|  |  |
| --- | --- |
| **A.18.2 Information security reviews** | |
| **Short description** | To ensure that information security is implemented and operated in  accordance with the organizational policies and procedures. |
| **ISO 27001 Control** | * + - 1. Independent review of information security       2. Compliance with security policies and standards       3. Technical compliance review |
| **Observations** | * QuickCover Insurance does not have the process of periodic independent review of opportunities for improvement and the need for changes to the approach to security. |
| **Observation**  **Ranking** | Major non-conformity |
| **Recommendations** | * Initiate the independent review of control objectives, controls, policies, processes and procedures for information security at planned intervals or when significant changes occur. * Review the compliance of information processing and procedures within each managers area of responsibility with the appropriate security policies, standards and any other security requirements.   If any non-compliance is found as a result of the review, managers should:   * + identify the causes of the non-compliance;   + evaluate the need for actions to achieve compliance;   + implement appropriate corrective action;   + review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses. * Review technical compliance to ensure that hardware and software controls have been correctly implemented. It covers penetration testing and vulnerability assessments, which might be carried out by |

|  |  |
| --- | --- |
|  | independent experts specifically contracted for this purpose. Such tests should be planned, documented and repeatable. |
| **Documents reviewed** | Not In place |

# SUMMARY

Within the scope of security assessment for QuickCover Insurance an interview with the Owner to examine current security level within organization and review existing documentation/policies. After mapping outcomes of interview and documentation analysis on ISO/IEC 27001:2013 controls, we evaluated current state of implemented Information Security Management Framework.

We recommend QuickCover Insurance to start implementing security controls one-by-one to raise them up to recommended level of maturity and in such way cover technical aspects of ISO/IEC 27001 compliance.[[1]](#footnote-1)

1. [↑](#footnote-ref-1)