Sri Lanka Institute of Information Technology

Enterprise Standards for Information security Assignment

Report on ISO 27001 Implementation for an Organization

IE3102– Enterprise Standards for Information security

Submitted by:

Student Registration Number	Student Name
IT20228880	K.K.K.P Kumara
IT20223144	P.I Chaminda

Contents

Overview

RedArms Security Company

RedArms security company is covering the all island wide security measures and its provide as the security of database, security that provide as the network and firewall in to the organizations and top leading companies. Its implement to secure the system and company important information. This can be related with the large companies that provide some services like IT and connection between the network. This can be the leading service provide company as well.

Introduction

The ISO framework is a set of guidelines that businesses can use to improve their operations. [1]ISO 27001 allows organizations of any size and in any industry to create an Information Security Management System to systematically and affordably safeguard the private information they store (ISMS). The standard equips businesses with the knowledge to safeguard their most sensitive data, and certification against it demonstrates to customers and business associates that the company takes data security seriously. Since ISO 27001 is accepted around the world, businesses and individuals who hold the certification have access to more lucrative markets.

An information [2] security management system must adhere to the guidelines outlined in ISO/IEC 27001. Rules for evaluating and responding to potential threats to an organization's information system are included. ISO/IEC 27001:2013's requirements are broad and apply to all types, sizes, and types of businesses. [3] Information Security Management Systems (ISMS) can be effectively implemented with the help of the guidelines provided by this standard. Through its safe and streamlined administration procedures, this framework ensures the confidentiality, integrity, and availability of data.

One of the most widely adopted and certified Information Security Standards is ISO 27001. This report delves deep into what ISO27001 Audit Controls are and how they can improve the company's Cyber Security and how to implement them on RedArms Security Company.

ISO 27001 Clauses

CLAUSE 1: Scope

CLAUSE 2: Normative references

CLAUSE 3: Terms and definitions

CLAUSE 4: Context of the organization

CLAUSE 5: Leadership

CLAUSE 6: Planning

CLAUSE 7: Support

CLAUSE 8: Operation

CLAUSE 9: Performance evaluation

CLAUSE 10: Improvement

Benefits

More than 40,000 businesses around the world have attained ISO 27001 Certification, making it the most widely adopted standard for information security. Organizations can improve their data security by adopting ISO 27001, a globally recognized standard. [4]

- Information stored in the Cloud, on paper, or anywhere else can be better protected by an information security management system that complies with ISO 27001.
- With the use of ISO 27001 Certification and a risk assessment and analysis approach, businesses can save money that would otherwise go toward potentially ineffective layers of protective technology.
- The ISO 27001 standard is deeply ingrained in the company's culture; employees are more cognizant of information security risks; and security procedures are pervasive across all areas of the business.
- Organizations can better adapt to evolving information security threats by adhering to ISO 27001's risk management guidelines.
- A company's vulnerability to cyberattacks and data breaches can be greatly mitigated through the establishment and upkeep of an information security management system.
- your information technology environment will likely experience a rise in the number of security breaches.
- Maintaining the information's privacy and confidentiality
- minimization of eleven risks, the possibility for their effects, and the associated costs
- competitive advantage resulting from well recognized standards
- Increase by 10 the number of partners, consumers, and members of the general public who are respected.
- Satisfaction of criteria that are generally acknowledged worldwide
- Identification of weaknesses in a methodical manner
- Reduced expenses
- Manage of IT risk
- Customers and other stakeholders will have more faith in your ability to manage risk if you do this.

ISMS (Information Security Management System) In ISO 27001

Primary Goal of ISMS : Minimize risks of business and ensure business continuity

Using an ISMS, you can explain and display how seriously your business takes data protection and privacy. It will aid in the detection and mitigation of risks and opportunities pertaining to your most prized data and associated assets. [5]That prevents security breaches and safeguards your business from disruption in the event that one does occur.

The requirements of an information security management system are specified in international security standard ISO 27001.

ISO 27001 and the best-practice principles contained in ISO 27002 are two good guides that can help you get started with the implementation of an information security management system (ISMS).

An ISMS must be independently audited by an approved certification body to ensure compliance with the ISO/IEC, according to the organization's standards.

The thoroughness of the information security risk assessment is essential to any implementation and, as a result, is directly correlated to the strength of an information security management system (ISMS).

ISO 27001 and the best-practice principles contained in ISO 27002 are two good guides that can help you get started with the implementation of an information security management system (ISMS).

Prior to implementing preventative measures, it is necessary to identify the full range of potential threats to the firm and its data ("controls").

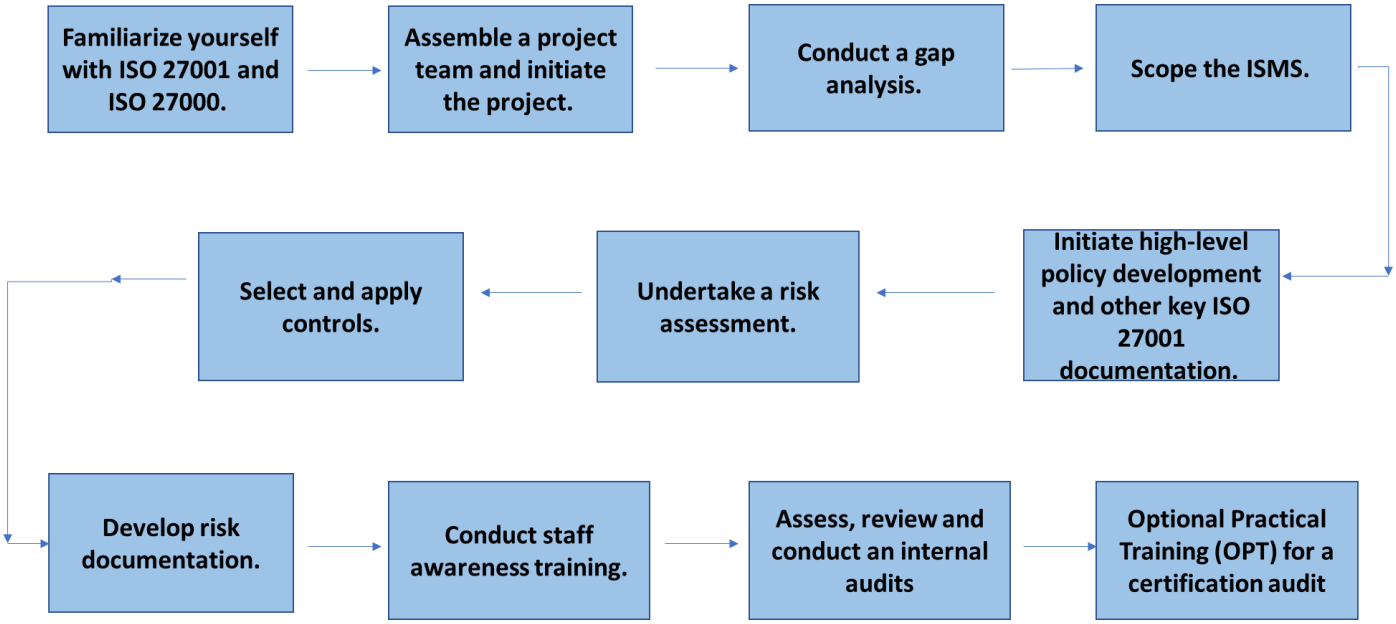
The international security standard ISO 27001 details the requirements that must be met by an information security management system.

ISO 27001 presents a list of recommended controls that might serve as a checklist for legislative, corporate, contractual, or regulatory objectives.

An ISMS must be independently audited by an approved certification body to ensure compliance with the ISO/IEC, according to the organization's standards. of an information security management system (ISMS).

Implementation of ISO 27001

Organization can be implemented this ISO 27001 with 11 steps



Step 01 : Familiarize yourself with ISO 27001 and ISO 27000.

As the first step team or you need to know and learn all aspects of standards and what can we do by implementing this and Organization should know the basics and importance.

Step 02 : Assemble a project team and initiate the project.

Then organization choose a team with members who have the knowledge and appointed a project leader according to cost and initiate the project immediately.

Step 03 : Conduct a gap analysis.

In order to identify insufficient methods, procedures, technology, or abilities, a gap analysis compares actual results to projected outcomes. In light of the results of a gap analysis, suggest changes that could help your company get closer to its ideal future state.

Step 04 : Scope the ISMS.

The scope of an ISMS will be determined to include only particular processes, services, and systems, as well as specific departments. The lessons learned from past successes can then be incorporated into a business case for either broadening the ISMS's scope or establishing a new, distinct scope with distinct prerequisites and safeguards.

As an examples, in RedArms Security Company should implement the standards for very critical departments and services with the cost analysis. This stage defines the scope of your ISMS and its daily impact.

You must know everything related to your organization so the ISMS can suit its needs .Defining the ISMS scope is crucial. This includes physical or digital files, systems, and portable devices. Defining your project's scope is crucial for ISMS deployment. If your scope is too small, you risk your organization's security. Too much scope will make the ISMS difficult to manage.

Step 05 : Initiate high-level policy development and other key ISO 27001 documentation.

A policy details purpose, ownership, duties and responsibilities, and linked papers or policies. Organizational policy is often the highest-level policy declaration from which all other policies, norms, guidelines, or processes receive validity. That kind of high level policy declaration is must and there are many documentations in ISO 27001 .Organization should pay attention to important documents amony them such as risk assessment report (clauses 8.2 and 8.3), Inventory of assets (clause A.8.1.1) etc.

Step 06 : Undertake a risk assessment.

In this step, Project team should do the risk assessment on the company with the scope. They should identify assets ,what are the risks in present and future .

Step 07 : Select and apply controls.

In this step, Team should select suitable controls for identified risks on previous step , Implementing the risk treatment strategy builds security safeguards to secure your organization's data. To ensure these measures are effective, confirm that employees can use them and knows their information security obligations.

Step 08 : Develop risk documentation.

Effective risk management relies on thorough documentation, which serves as both a delivery and communication channel. Uncertainty surrounds us. With this in mind, risk management will guide our choices and, depending on the level of development of the program, may even provide a strategic advantage.

Step 09 : Conduct staff awareness training.

Weakest link of the cyber security is the human. Without the knowledge of these things ,Any controls that we implement for secure systems are useless .So Staff awareness training is must. Staff induction is the first step in what should be a continuous process of raising awareness among employees, which should be supplemented with additional reminders and refreshers

throughout the year and especially after any security events involving employees. An effective employee awareness program has the following benefits: It aids businesses in discovering vulnerabilities in their security measures.

Step 10 : Assess, review and conduct an internal audits

Internal Audit is a group or division within a firm that conducts objective, third-party examinations of operational structures and procedures. [6] An internal audit department is responsible for giving top management and board members impartial information. Top management need to test controls that team have implemented and They should work properly.

Step 11 : Optional Practical Training (OPT) for a certification audit

The certification body you use should be properly accredited by a recognized regional accreditor body and a member of the international accreditation forum. Your chosen certification body reviews your management system documentation. Check that you have implemented appropriate control and conductors .to audit in order to put the procedure to the test in practice.

Toolkit Documents

1. IS027k Model policy on change management and control
2. Business Case
3. Data restoration form
4. Information classification matrix
5. IS027k ISM organization chart data
6. S027k ISMS internal audit procedure v3
7. IS027k SOA 2013 English and Spanish updated
8. Nonconformity corrective preventive action form
9. Risk Assessment

01.Business Case

ISO/IEC 27001 compliance certifies that a company has adopted ISO27k to manage information risks. Certification demonstrates that a company has passed the compliance obstacle (the yardstick) and invests in a compliant ISMS. [7]

Click here to view Document

ISO 27001 security

Business case for an Information Security Management System (ISMS) based on the ISO/IEC 27000 series standards (ISO27k) for RedArms Security Company

Executive summary

Benefits

The ISMS will place Information security under strict management supervision, allowing for guidance and Improvement where necessary. Improved Information security reduces the risk (of occurrence and/or negative consequences) of events, lowering incident-related losses and expenses.

Other Benefits,

- A organized, consistent, and professional approach to Information security management, in line with other ISO management systems
- Demonstrable governance utilizing globally known good security practices
- Comprehensive information security risk assessment and treatment according to business and security priorities

Costs

Because information security is a business and compliance need, the majority of the expenses associated would be expended anyhow. The following are the specific expenses associated with the ISMS: • Resources required to develop, implement, and run the ISMS, including project management for the implementation project

- Various company processes and activities must be changed to confirm ISO standards
- Third-Party compliance audits(optional -only necessary if we chose to pursue certification which we may do after the ISMS is up and running

Introduction, scope and purpose

RedArms Security Is an island-wide company which provides Database Security, Network Security. Firewall Implementing to leading companies.

Scope is to survive Serendib from cyber treats to protect confidential and sensitive data from other parties and the Purpose is using Organizational Informational Security Management Systems (ISMS) will be helpful to ensure that they are following information security laws and regulations.

ISMS benefits

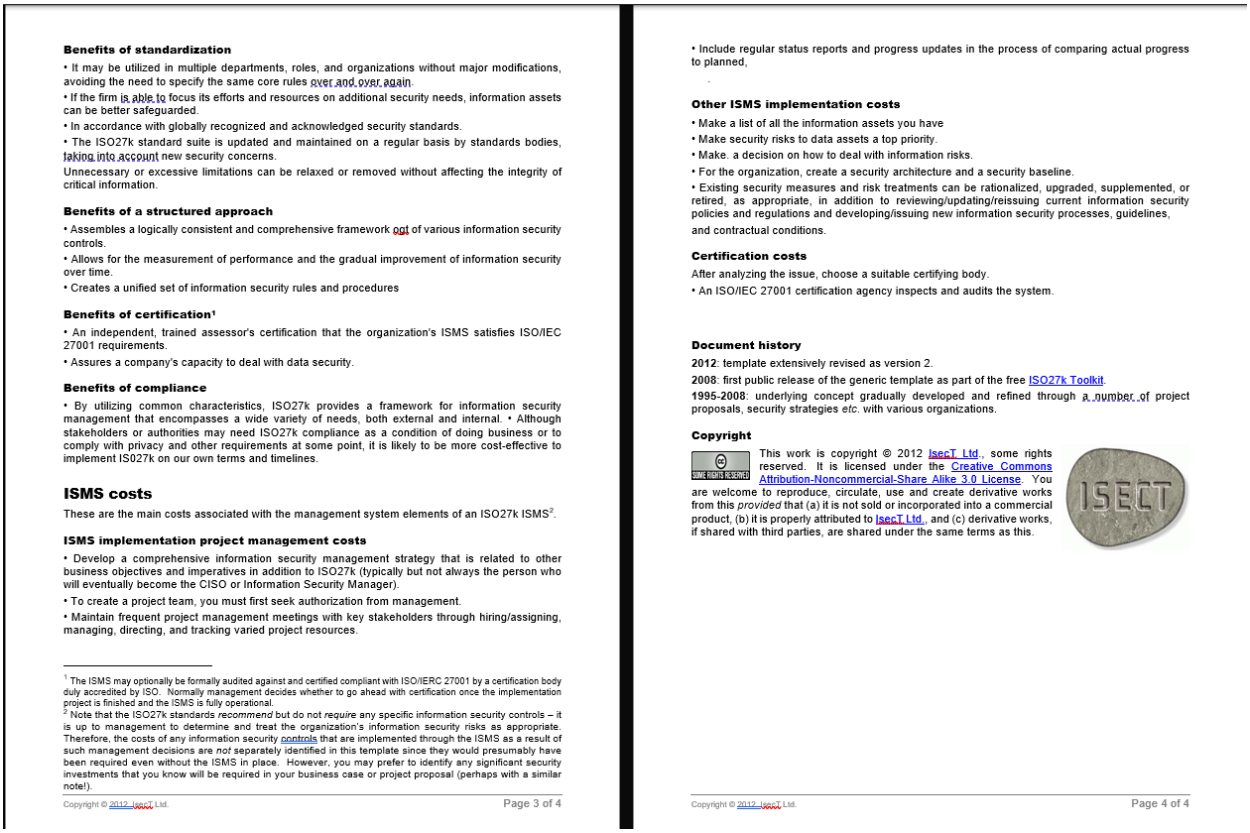
These are the ways in which an ISO27k ISMS will typically benefit the organization.

Information security risk reduction

• Using a thorough, well-structured process, all relevant information security risks, vulnerabilities, and impacts are more likely to be discovered, assessed, and treated effectively.

• This approach ensures consistency across various information communications systems (ICT) and corporate processes, while also tackling information security risks in order of importance.

• They get a better understanding of information security terms, hazards, and controls



Benefits of standardization

• It may be utilized in multiple departments, roles, and organizations without major modifications, avoiding the need to specify the same core rules over and over again.

• If the firm is able to focus its efforts and resources on additional security needs, information assets can be better safeguarded.

• In accordance with globally recognized and acknowledged security standards.

• The ISO27k standard suite is updated and maintained on a regular basis by standards bodies, taking into account new security concerns.

Unnecessary or excessive limitations can be relaxed or removed without affecting the integrity of critical information.

Benefits of a structured approach

• Assembles a logically consistent and comprehensive framework out of various information security controls.

• Allows for the measurement of performance and the gradual improvement of information security over time.

• Creates a unified set of information security rules and procedures

Benefits of certification[1]

• An independent, trained assessor's certification that the organization's ISMS satisfies ISO/IEC 27001 requirements.

• Assures a company's capacity to deal with data security.

Benefits of compliance

• By utilizing common characteristics, ISO27k provides a framework for information security management that encompasses a wide variety of needs, both external and internal. • Although stakeholders or authorities may need ISO27k compliance as a condition of doing business or to comply with privacy and other requirements at some point, it is likely to be more cost-effective to implement IS027k on our own terms and timelines.

ISMS costs

These are the main costs associated with the management system elements of an ISO27k ISMS[2].

ISMS implementation project management costs

• Develop a comprehensive information security management strategy that is related to other business objectives and imperatives in addition to ISO27k (typically but not always the person who will eventually become the CISO or Information Security Manager).

• To create a project team, you must first seek authorization from management.

• Maintain frequent project management meetings with key stakeholders through hiring/assigning, managing, directing, and tracking varied project resources.

[1] The ISMS may optionally be formally audited against and certified compliant with ISO/IERC 27001 by a certification body duly accredited by ISO. Normally management decides whether to go ahead with certification once the implementation project is finished and the ISMS is fully operational.

[2] Note that the ISO27k standards *recommend* but do not *require* any specific information security controls – it is up to management to determine and treat the organization's information security risks as appropriate. Therefore, the costs of any information security controls that are implemented through the ISMS as a result of such management decisions are *not* separately identified in this template since they would presumably have been required even without the ISMS in place. However, you may prefer to identify any significant security investments that you know will be required in your business case or project proposal (perhaps with a similar note!).

Copyright © 2012 IsecT Ltd. Page 3 of 4

• Include regular status reports and progress updates in the process of comparing actual progress to planned,

Other ISMS implementation costs

• Make a list of all the information assets you have

• Make security risks to data assets a top priority.

• Make. a decision on how to deal with information risks.

• For the organization, create a security architecture and a security baseline.

• Existing security measures and risk treatments can be rationalized, upgraded, supplemented, or retired, as appropriate, in addition to reviewing/updating/reissuing current information security policies and regulations and developing/issuing new information security processes, guidelines, and contractual conditions.

Certification costs

After analyzing the issue, choose a suitable certifying body.

• An ISO/IEC 27001 certification agency inspects and audits the system.

Document history

2012: template extensively revised as version 2.

2008: first public release of the generic template as part of the free ISO27k Toolkit.

1995-2008: underlying concept gradually developed and refined through a number of project proposals, security strategies *etc.* with various organizations.

Copyright

Copyright © 2012 IsecT Ltd. Page 4 of 4

02.Assest Register

According to ISO 27001. an asset is any valued location within an organization's systems where confidential information is kept, processed, or accessed. Any equipment owned by an employee, such as a desktop, laptop, or corporate phone, is an asset. Additionally, the assets represented by the private data kept on those devices.

Code, name, description, capitalization date, cost, department, cost center, residual value, asset life, and depreciation rule are all examples of the kind of details typically recorded in a fixed asset register.

[Click here to view Document]

Asset Register

Version: 1

Entity	Asset Group	Asset Type	Description (including examples)	Risk Owner	Risk Owner Name
Applications	Customer Data	Information	Personal informations of the bank customers	Product Manager	Mr. Yasiru Pathirana
Finance	Financial data	Information	Financial Data of the bank customers	CFO	Mr. Kasun Chanaka
Facilities	Premises	Building	Premises, reception, fixture & fittings, alarms, CCTV, data processing areas	Chief Branch Manager	Mr. Dasun Dissanayaka
HR	Staff Data	People	Personal data of Company Staff (Directors, Supervisors, Operational staff, temps, contractors)	HR Manager	Mr. Uditha Perera
IT	Desktops / Laptops	Hardware	Office staff workstations (includes keyboard, mouse, screen, PCs, thin clients etc)	Internal IT	Mr.Supun Silva
IT	Removable Media	Hardware	USB stick; CDs, Portable Hard drives...	Internal IT	Mr.Supun Silva
IT	Server room (Internal)	Building	Room where servers are held	Internal IT	Mr.Supun Silva
IT	Servers (Internal)	Hardware	Exchange, File, File & print, FTP, webservers, Domain Controllers	Internal IT	Mr.Supun Silva
IT	Purchased Software	Software	Software employed; graphics; HR and associated licences etc.	Internal IT	Mr.Supun Silva
IT	Telecommunications	Services	Landline/Fixed Phones; faxes	Internal IT	Mr.Supun Silva
IT	Backups	Hardware	Backups of company held information (tapes, discs, server etc.)	IT Operations	Ms. Ruwani Ranasinghe
IT	Servers (Datacenter)	Hardware	Customer products and applications.	IT Operations	Ms. Ruwani Ranasinghe
IT	Websites (Public)	Information	Company owned public websites	CTO	Ms. Isuri Liyanarachchi
IT	Web Application	Information	Online Banking Web Application Of the Company	CTO	Ms. Isuri Liyanarachchi

Doc Control | Assets | Assets Detail

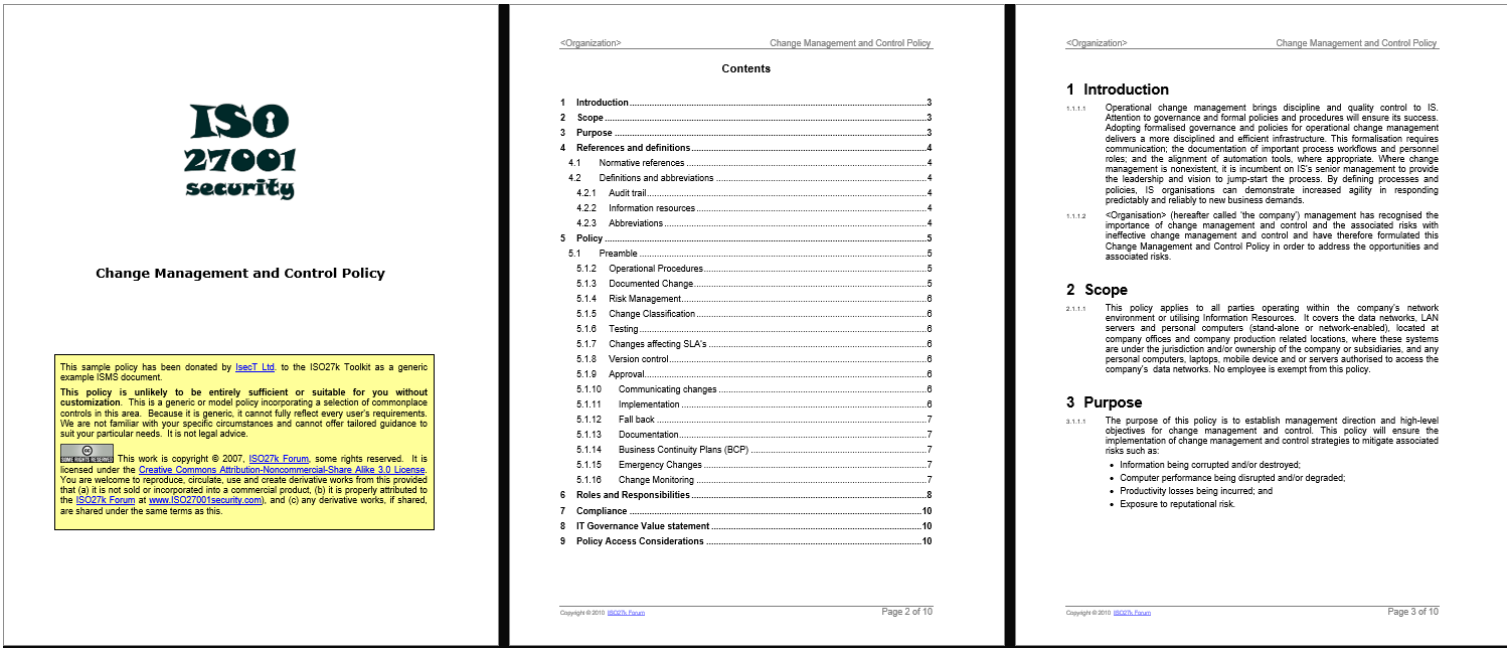
Entity	Asset Group	Classification	Data Classification	Asset ID	Assigned To	Employee ID	Assigned Date	Return Date
Laptop	HP Pavilion x360 Convertible	Hardware	Confidential	A0001	Jayantha karunarathne	E1156	6/5/2020	
Laptop	HP Pavilion x360 Convertible	Hardware	Confidential	A0002	Ashan priyashan	E1157	6/5/2020	
Laptop	HP Pavilion x360 Convertible	Hardware	Confidential	A0003	Samantha premalal	E1158	6/5/2020	
Laptop	HP Pavilion x360 Convertible	Hardware	Confidential	A0004	Tishan senevirathe	E1159	6/5/2020	10/8/2020
Laptop	HP Pavilion x360 Convertible	Hardware	Confidential	A0005	Priyashan jayalath	E1160	6/5/2020	
Monitor	HP V24i FHD Monitor	Hardware	n/a	A0006	Dinuka gamlath	E1157	6/5/2020	
Monitor	HP V24i FHD Monitor	Hardware	n/a	A0007	Renuka mithsara	E1158	6/5/2020	
Monitor	HP V24i FHD Monitor	Hardware	n/a	A0008	Pawara hirushan	E1159	6/5/2020	10/8/2020
Monitor	HP V24i FHD Monitor	Hardware	n/a	A0009	Anura shamal	E1160	6/5/2020	
Colombo	n/a	Physical	Company Secret	1	Gishan gunasena	E1005	1/1/2015	
City Office	n/a	Physical	Company Secret	2	Hirun nethmal	E1005	1/1/2015	

Doc Control | Assets | Assets Detail

03.ISO27k Model policy on change management and control

A change management policy should define step-by-step system adjustments. An RFC (Request for Change) is the initial stage in requesting a change. [8]The RFC should record the requester, the date, and the applicable department or party. From there, a delegated employee analyzes the RFC and identifies the change's effects on the organization. This includes not just the changes themselves, but also their economic impact and information security issues. Employee provides RFC and analysis to change implementer. The IT manager or a Change Manager could do this. This individual will examine the change's internal and external impacts, including regulatory compliance, operational effectiveness, and information security (such as predicted customer response and the effect the change will have on the supply chain).The employee will approve or reject the RFC based on this information. If they chose the former, it will be submitted to the change planner to complete the process. That's probably a department or project head. In smaller organizations, one individual may handle many change management tasks. This is a valid strategy to manage change, but each step must be documented.

Click here to view document



ISO 27001 security

Change Management and Control Policy

This sample policy has been donated by IsecT Ltd. to the ISO27k Toolkit as a generic example ISMS document.

This policy is unlikely to be entirely sufficient or suitable for you without customization. This is a generic or model policy incorporating a selection of commonplace controls in this area. Because it is generic, it cannot fully reflect every user's requirements. We are not familiar with your specific circumstances and cannot offer tailored guidance to suit your particular needs. It is not legal advice.

This work is copyright © 2007, ISO27k Forum, some rights reserved. It is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this provided that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k Forum at www.ISO27001security.com), and (c) any derivative works, if shared, are shared under the same terms as this.

Contents

1 Introduction

1.1.1.1 Operational change management brings discipline and quality control to IS. Attention to governance and formal policies and procedures will ensure its success. Adopting formalised governance and policies for operational change management delivers a more disciplined and efficient infrastructure. This formalisation requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate. Where change management is nonexistent, it is incumbent on IS's senior management to provide the leadership and vision to jump-start the process. By defining processes and policies, IS organisations can demonstrate increased agility in responding predictably and reliably to new business demands.

1.1.1.2 <Organisation> (hereafter called 'the company') management has recognised the importance of change management and control and the associated risks with ineffective change management and control and have therefore formulated this Change Management and Control Policy in order to address the opportunities and associated risks.

2 Scope

2.1.1.1 This policy applies to all parties operating within the company's network environment or utilising Information Resources. It covers the data networks, LAN servers and personal computers (stand-alone or network-enabled), located at company offices and company production related locations, where these systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device and or servers authorised to access the company's data networks. No employee is exempt from this policy.

3 Purpose

3.1.1.1 The purpose of this policy is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

- Information being corrupted and/or destroyed;
- Computer performance being disrupted and/or degraded;
- Productivity losses being incurred; and
- Exposure to reputational risk.

4 References and definitions

4.1 *Normative references*

4.1.1.1 The following documents contain provisions that, through reference in the text, constitute requirements of this policy. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this policy are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

- Information Security Policy (overall)
- Information Security - Systems Development and Maintenance Policy
- Information Security - Business Continuity Management
- Information Security - Physical Asset Classification and Control Policy
- Information Security – Change Control Procedure

4.2 *Definitions and abbreviations*

4.2.1 Audit trail

4.2.1.1 A record or series of records which allows the processing carried out by a computer system to be accurately identified, as well as verifying the authenticity of such amendments.

4.2.2 Information resources

4.2.2.1 All data, information as well as the hardware, software, personnel and processes involved with the storage, processing and output of such information. This includes data networks, servers, PC's, storage media, printer, photo copiers, fax machines, supporting equipment, fall-back equipment and back-up media.

4.2.3 Abbreviations

- PC: Personal Computer
- BCP: Business Continuity Plan
- SLA: Service Level Agreement

5 Policy

5.1 *Preamble*

5.1.1.1 Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.

5.1.1.2 In order to fulfil this policy, the following statements shall be adhered to:

5.1.2 Operational Procedures

5.1.2.1 The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical company information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.

5.1.2.2 At a minimum the change control process should include the following phases:

- Logged Change Requests;
- Identification, prioritisation and initiation of change;
- Proper authorisation of change;
- Requirements analysis;
- Inter-dependency and compliance analysis;
- Impact Assessment;
- Change approach;
- Change testing;
- User acceptance testing and approval;
- Implementation and release planning;
- Documentation;
- Change monitoring;
- Defined responsibilities and authorities of all users and IT personnel;
- Emergency change classification parameters.

5.1.3 Documented Change

5.1.3.1 All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.

5.1.3.2 A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.

5.1.4 Risk Management

5.1.4.1 A risk assessment shall be performed for all changes and dependant on the outcome, an impact assessment should be performed.

5.1.4.2 The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

5.1.5 Change Classification

5.1.5.1 All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.

5.1.6 Testing

5.1.6.1 Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made. (For more information see **System Development Life Cycle** [citation here]).

5.1.7 Changes affecting SLA's

5.1.7.1 The impact of change on existing SLA's shall be considered. Where applicable, changes to the SLA shall be controlled through a formal change process which includes contractual amendments.

5.1.8 Version control

5.1.8.1 Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies. (For more information see **System Development Life Cycle** [citation here])

5.1.9 Approval

5.1.9.1 All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.

5.1.10 Communicating changes

5.1.10.1 All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

5.1.11 Implementation

5.1.11.1 Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes. (For more information see **System Development Life Cycle** [citation here])

5.1.12 Fall back

5.1.12.1 Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

5.1.13 Documentation

5.1.13.1 Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.

5.1.13.2 Information resources documentation is used for reference purposes in various scenarios i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer and/or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes. Policies and procedures, affected by software changes, shall be updated on completion of each change.

5.1.14 Business Continuity Plans (BCP)

5.1.14.1 Business continuity plans shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy and availability of BCP documentation. BCP documentation is the road map used to minimise disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.

5.1.15 Emergency Changes

5.1.15.1 Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.

5.1.16 Change Monitoring

5.1.16.1 All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

6 Roles and Responsibilities

ROLE	FUNCTIONAL RESPONSIBILITIES
Members of the Board	• Members of the Board shall ensure that the necessary information security controls are implemented and complied with as per this policy.
Information Security Manager	• Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and subsidiaries; • Facilitate and co-ordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards; • Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products; • Co-ordinate the overall communication and awareness strategy for change management; • Acts as the management champion for change management and control; • Provide technical input to the service requirements and co-ordinate affected changes to SLA's where applicable. • Establish and co-ordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives; and • Co-ordinate the implementation of new or additional security controls for change management.
Operations Manager	• Implement, maintain and update the change management and control strategy, baselines, standards, policies and procedures with input from all stakeholders; • Approve and authorise change management and control measures on behalf of the <Organisation>; • Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control; • Ensure that policy, standards and procedural changes are communicated to applicable owners and management forums; • Appoint the necessary representation to the interest groups and other forums created by each company for Information Security Management relating to change management and control;

	• Establish and revise the information security strategy, policy and standards for change management and control; • Facilitate and co-ordinate the necessary change management and control initiatives within each company; • Report and evaluate changes to change management and control policies and standards; • Co-ordinate the overall communication and awareness strategy for change management and control; • Co-ordinate the implementation of new or additional security controls for change management and control • Review the effectiveness of change management and control strategy and implement remedial controls where deficits are identified; • Provide regular updates on change management and control initiatives and the suitable application; • Evaluate and recommend changes to change management/ version control solutions; and • Co-ordinate awareness strategies and rollouts to effectively communicate change management and control mitigation solutions in each company. • Establish and implement the necessary standards and procedures that conform to the Information Security policy; • Responsible for approving, authorising, monitoring and enforcing change management initiatives and related security controls within all <ORGANISATION> companies and divisions; • Ensure that all solution owners are aware of policies, standards, procedures and guidelines for change management and control. • Ensure the compliance of this policy and report deviations to the Information Manager.
IT Service Provider	• Shall comply with all change management and control statements of this policy.
Solution Owners	• Shall comply with all information security policies, standards and procedures for change management and control; and • Report all deviations.

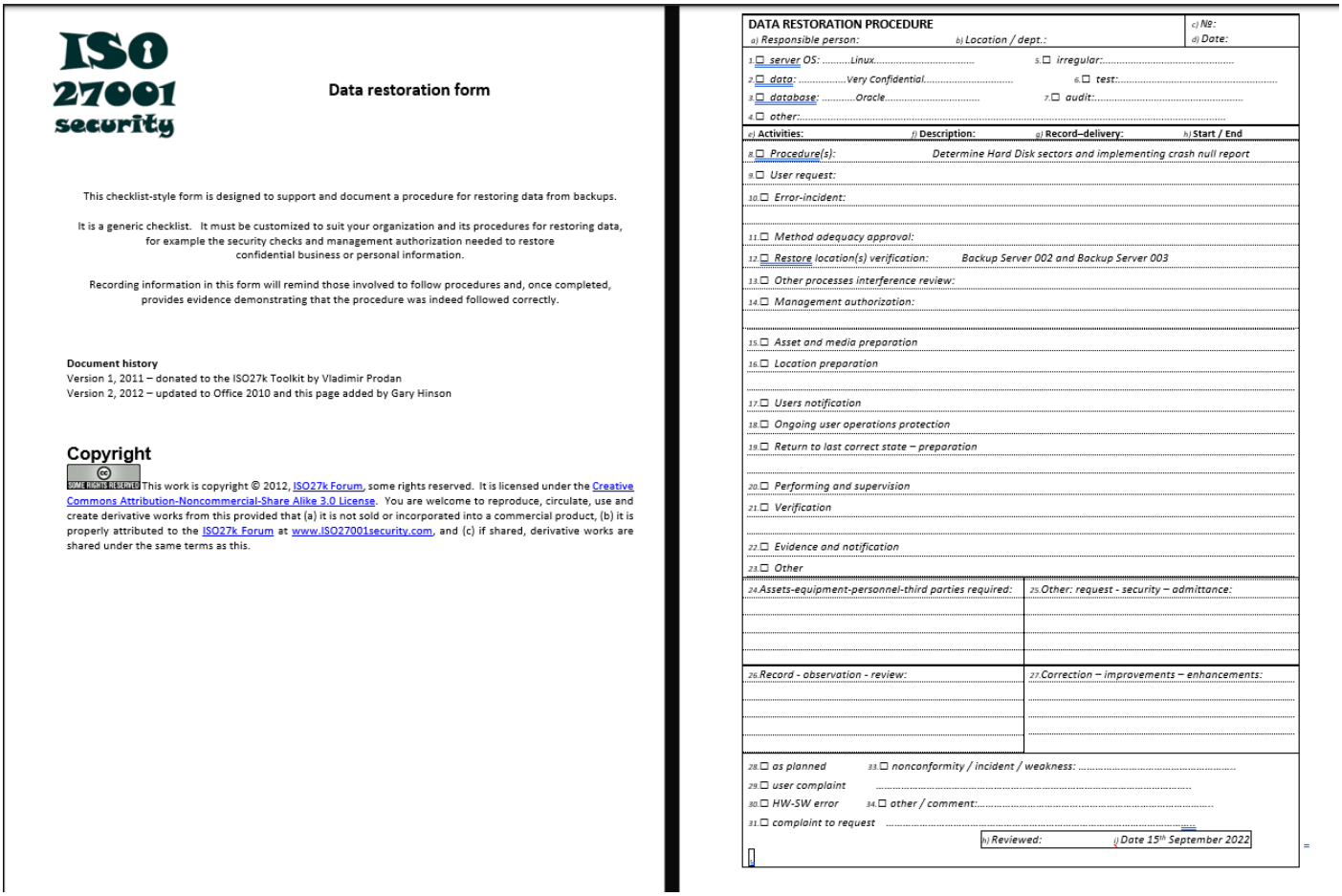
Table 1 Roles and Responsibilities

04.Data restoration form

Planned backup failures should be addressed to ensure all backups match policy. Reviewing continuity plans periodically ensures that backup procedures meet business standards. All data, software, and information needed to restore the network should be backed up. Consider if archive copies will be kept permanently when setting a preservation period.

Team should use data restoration form fill and team have completed the form like following figure

Click here to view document



ISO 27001 security

Data restoration form

This checklist-style form is designed to support and document a procedure for restoring data from backups.

It is a generic checklist. It must be customized to suit your organization and its procedures for restoring data, for example the security checks and management authorization needed to restore confidential business or personal information.

Recording information in this form will remind those involved to follow procedures and, once completed, provides evidence demonstrating that the procedure was indeed followed correctly.

Document history
Version 1, 2011 – donated to the ISO27k Toolkit by Vladimir Prodan
Version 2, 2012 – updated to Office 2010 and this page added by Gary Hinson

Copyright
SOME RIGHTS RESERVED This work is copyright © 2012, ISO27k Forum, some rights reserved. It is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this provided that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k Forum at www.ISO27001security.com, and (c) if shared, derivative works are shared under the same terms as this.

DATA RESTORATION PROCEDURE
a) Responsible person: b) Location / dept.: c) №: d) Date:

1. ☐ server OS: .....Linux..... 5. ☐ irregular:.....
2. ☐ data: .....Very Confidential..... 6. ☐ test:.....
3. ☐ database: .....Oracle..... 7. ☐ audit:.....
4. ☐ other:.....

e) Activities: f) Description: g) Record–delivery: h) Start / End

8. ☐ Procedure(s): Determine Hard Disk sectors and implementing crash null report
9. ☐ User request:
10. ☐ Error-incident:
11. ☐ Method adequacy approval:
12. ☐ Restore location(s) verification: Backup Server 002 and Backup Server 003
13. ☐ Other processes interference review:
14. ☐ Management authorization:
15. ☐ Asset and media preparation
16. ☐ Location preparation
17. ☐ Users notification
18. ☐ Ongoing user operations protection
19. ☐ Return to last correct state – preparation
20. ☐ Performing and supervision
21. ☐ Verification
22. ☐ Evidence and notification
23. ☐ Other

24. Assets-equipment-personnel-third parties required:
25. Other: request - security – admittance:
26. Record - observation - review:
27. Correction – improvements – enhancements:

28. ☐ as planned
29. ☐ user complaint
30. ☐ HW-SW error
31. ☐ complaint to request
33. ☐ nonconformity / incident / weakness: .....
34. ☐ other / comment:.....

i) Reviewed: j) Date 15th September 2022

05.S027k ISMS internal audit procedure v3

The purpose of an internal audit against ISO 27001 is to determine whether or not your organization's ISMS satisfies the requirements of the Standard. [9]In contrast to a certification review, this one is carried out in-house and the findings used to shape how the ISMS moves forward. In clause 9.2 of ISO 27001, you'll find the guidelines for conducting an internal audit. Internal ISO 27001 audits ensure the management system and procedures comply with the Standard. It also ensures that processes are communicated, understood, and performed efficiently within the organization. The audit determines non-conformities, ISMS effectiveness, and opportunities for improvement.

Click here to view document

Internal audit benefits

- Find deviations from the standard before they are found by others.
- Maintain a high level of security by foreseeing any weak spots and fixing them in advance.
- Create a record of management's dedication and share it with them
- Incorporate staff comprehension and sensitivity
- Input for on-going enhancement

ISO 27001 security

Model
ISMS Internal Audit Procedure

Document Number:	2346
Version:	2
Release Date:	September 15th 2022
Document Owner:	Kumara K.K.K.P & Chaminda P.I

Document History

Version	Date	Author	Update Description
0	March 2022	W R Anuja Silva	Initial issue.
1	May 2022	S P Supun Krishantha	Updated Documentation Administration for incorporation into the ISO27k Toolkit
2	September 2022	R A Lasantha	Reformatted using styles plus minor updates to the wording here and there

1 Purpose of this procedure

1.1 To ensure that the company continually operates in accordance with the specified policies, procedures and external requirements in meeting company goals and objectives in relation to information security.

1.2 Also to ensure that improvements to the Information Security Management System (ISMS) are identified, implemented and suitable to achieve objectives.

2 Scope

2.1 This procedure includes planning, execution, reporting and follow–up of ISMS internal audits and applies to all departments and business units within scope of the organization's ISMS.

3 Rôles and responsibilities

3.1 Information Security Management Representative (ISMR)

- Appoints the Lead Auditor and the Audit Team (note: the Lead Auditor and ISMR may be the same person).
- Together with the Lead Auditor, reviews the corrective and preventive actions and the follow-up audits done based on the internal audit report submitted.
- Maintains the confidentiality of the audit results.

3.2 Lead Auditor

- Prepares an Audit Plan/Notification as a basis for planning the audit and for disseminating information about the audit.
- Leads the ISMS internal audit activities
- Co-ordinates the audit schedule with concerned department/section heads
- Plans the audit, prepares the working documents and briefs the audit team.
- Consolidates all audit findings and observations and prepares internal audit report.
- Reports critical non-conformities to the auditee immediately.
- Report to the auditee the audit results clearly and without delay.
- Conducts the opening and closing meeting.

3.3 Audit Team Member

- Supports the Lead Auditor's activities.
- Performs the audit using the consolidated audit checklist.
- Reports the non-conformities and recommends suggestions for improvement
- Retains the confidentiality of audit findings.
- Acts in an ethical manner at all times.

3.4 Auditee

- Receives, considers and discusses the audit report.
- Determines, resources, drives and completes corrective actions as necessary.
- Is and remains accountable for protecting information assets.

4 Procedure

4.1 General

4.1.1 An ISMS audit programme shall be created that contains all scheduled and potential audits for the whole calendar year. This shall include schedule of internal audits, audits of suppliers, audits to be performed by clients and third-party audits, as appropriate.

4.1.2 Internal audits shall be scheduled twice a year or as the need arises.

4.1.3 Only competent personnel who are truly independent of the subject area shall perform audits.

4.1.4 All members of the Internal Audit Team shall be appointed by the ISMR

4.1.5 The Lead Auditor shall supervise the activity of the Audit Team.

4.1.6 An Audit Notification Memo is sent to the department/section to be audited at least three working days in advance of the audit.

4.2 Planning and Preparing the Audit

4.2.1 An annual ISMS internal audit programme shall be prepared by the Lead Auditor and approved by the President or CEO. It should be revised to reflect any changes in the priorities or schedule during the year.

4.2.2 Based on the audit programme, the Lead Auditor shall prepare the respective audit plans.

4.2.3 The Audit Plan/Notification shall be prepared by the Lead Auditor, reviewed and approved by the ISMR. It shall be communicated to the auditors and the auditees. It shall be designed to be flexible in order to permit changes based on the information gathered during the audit. The plan shall include:

- Audit objective and scope
- Department/Section and responsible individuals in charge.
- Audit team members. The number of auditors depends on the audit area size.
- Type of management system to be audited
- Date, place, time of the audit and distribution date of the audit report

4.3 Pre-audit meeting

4.3.1 One or more pre-audit meetings between the ISMR, Lead Auditor and auditors shall take place not later than one day prior to the audit proper. Objectives are as follows:

- To ensure the availability of all the resources needed and other logistics that may be required by the auditor.
- The scope of the audit is verified from the Audit Plan

4.4 Opening meeting

4.4.1 An opening meeting, where deemed appropriate by the ISMR and Lead Auditor, shall be held on the day of the audit but before the audit proper. The following may be discussed during the opening meeting:

- The purpose and scope of the audit.
- Confirmation of the audit plan

- Clarification of other matters must be settled before the audit takes place.

4.5 Audit Execution

4.5.1 The auditors will perform the internal audit using several checklists:
- Internal Audit Checklist/Observation Form – contains specific items that are particular to the organizational unit to be audited. The assigned auditors are responsible for generating questions using this form.
- Systemic Requirements Checklist– contain items relating to the requirements of ISO/IEC 27001:2005
- Control Requirements Checklist– contain items pertaining to controls outlined in Appendix A of ISO/IEC 27001:2005 and described more fully in ISO/IEC 27002:2005.

4.5.2 Audit findings are collected through interviews, examination of documents and observation of activities and conditions in the areas of concern and will be written on the above-mentioned checklists.

4.5.3 Evidence suggesting other non-conformities should be noted if they seem significant, even though not covered by the checklist. Other objective evidence and/or observations that may reflect positively or negatively on the information security management system shall also be listed on the space provided for on the above-mentioned checklists.

4.6 Audit Reporting

4.6.1 The auditors shall have a wash-up meeting after the audit. Agenda includes:
- Review and analysis of findings
- Consolidation of all findings including grouping and tabulation.
- Classification of findings.
- Preparation of recommendation and audit report
- Classification of findings (see section 4.6.4)
- Preparation of recommendation and audit report

4.6.2 The audit team shall review all of their findings whether they are to be reported as non-conformities or as observations. Audit finding should likewise be supported by objective evidence.

4.6.3 The Lead Auditor consolidates all the audit findings for the preparation of the audit report.

4.6.4 Classification of findings shall be:
- **Major non-conformity** – This pertains to a major deficiency in the ISMS. A non-conformity also pertains to one or more element of the ISO 27001 is not implemented. Non-conformities have a direct affect on information security specifically on the preservation of confidentiality, integrity and availability of information assets.
- **Minor non-conformity** – A minor deficiency. One or more elements of the ISMS is/are only partially complied. Minor non- conformity has an indirect effect on information security.

Note: Both major and minor non-conformities require appropriate <u>corrective actions</u> to be documented on the NCPAR form.
- Improvement potential – A hint for improvement which may or may not be implemented by the auditee.

Note: Improvement potentials which pertain to an information security weakness shall require appropriate <u>preventive actions</u> to be documented on the NCPAR form.
- Positive findings – Findings that pertain to processes and/or systems that go beyond what is required by the standard.

4.6.4 The Lead Auditor shall prepare a standard internal audit Report containing the following information:
- Audit Reference Number
- Date of Audit
- Department/Section Audited/Process Name
- Name of Auditee and auditors
- Statement of findings (all non conformities found)

- Reference to the information security management system and standard
- Corrective and Preventive Actions with completion date
- Follow-up actions for non conformities
- Verification of follow-up actions

4.6.5 Auditors shall follow a code of conduct in the manner of reporting as stated in this document:
- The report should be concise but factual and presented in a constructive manner.
- The findings should be within the scope of audit and shows the relationship of the standard used.
- The report should not show bias by the individual auditor.

4.6.6 The Lead Auditor shall issue a formal Audit Report to the ISMR (if the ISMR is not the Lead Auditor).

4.6.7 The internal audit report shall be maintained and controlled by the ISMR in accordance with the **Control of Records Procedure.**

4.7 Closing Meeting

4.7.1 The Lead Auditor shall preside over the closing meeting attended by the audit team and the auditees.

4.7.2 The auditors shall report their findings, observations and recommendations, summarising the good points before discussing non-conformities supported by the audit evidence.

4.7.3 All parties shall safeguard the confidentiality of the internal audit report.

5 Audit Follow-up and Closure

5.1.1 Whereas the auditors are responsible for identifying non-conformities, auditees are responsible for resolving non-conformities.

5.1.2 Approved corrective actions shall be based on time scales agreed with the auditors.

5.1.3 The Lead Auditor shall follow-up to check the implementation of corrective action as stated on the Non-conformity/Corrective and Preventive Action report or NCPAR. Normally, follow-ups will use an abbreviated form of this audit procedure to verify the completion and effectiveness of the agreed corrective or preventive actions according to the agreed timescales.

5.1.4 The lead auditor shall issue a new NCPAR if corrective actions are not fully implemented by the committed date, and/or are not effective.

5.1.5 "Re-issue" shall be noted on the remarks column of the NCPAR log if any of the situations noted here become apparent.

5.1.6 An audit will not be considered complete and closed until all corrective actions or measures have been successfully implemented to the satisfaction of the Lead Auditor.

6 Auditors' Qualifications

6.1 Personal attributes

6.1.1 Auditors shall possess the personal attributes, skills and competencies necessary to uphold the principles of auditing. An auditor should be:
- Ethical *i.e.* fair, truthful, sincere, honest and discreet;
- Open-minded *i.e.* willing to consider alternative ideas or points of view;
- Diplomatic *i.e.* tactful in dealing with people, particularly those who are senior or over-committed;
- Observant *i.e.* actively aware of physical surroundings and activities;
- Perceptive, *i.e.* instinctively aware of and able to understand situations;
- Versatile *i.e.* able to adjust readily to different situations;

- Tenacious *i.e.* persistent, focused on achieving objectives;
- Decisive *i.e.* reaches timely conclusions based on logical reasoning and analysis; and
- Self-reliant *i.e.* acts and functions independently while interacting effectively with others.

6.2 General knowledge and skills of an ISMS auditor. Auditors should have knowledge and skills in the following areas.

6.2.1 **Audit principles, procedures and techniques**: to enable the auditor to apply those appropriate to different audits and ensure that audits are conducted consistently and systematically. An auditor should be able to:
- Apply audit principles, procedures and techniques;
- Plan and organize the work effectively;
- Conduct the audit within the agreed time schedule;
- Prioritize and focus on matters of significance;
- Collect information through effective interviewing, listening, observing and reviewing documents, records and data;
- Understand the appropriateness and consequences of using sampling techniques for auditing;
- Verify the accuracy of collected information;
- Confirm the sufficiency and appropriateness of audit evidence to support audit findings and conclusions;
- Assess those factors that can affect the reliability of the audit findings and conclusions;
- Use work documents to record audit activities;
- Prepare audit reports of suitable quality and professionalism;
- Maintain the confidentiality and security of information, and
- Communicate effectively, either through personal linguistic skills or through an interpreter.

6.2.2 Management system and reference documents: to enable the auditor to comprehend the scope of the audit and apply audit criteria. Knowledge and skills in this area should cover:
- Interaction between the parts of the management system;
- ISMS standards, applicable procedures or other documents used as audit criteria;
- Recognizing differences between and priority of the reference documents;
- Application of the reference documents to different audit situations, and
- Information systems and technology for, authorization, security, distribution and control of documents, data and records.

6.2.3 **Organization/business context**: to enable the auditor to comprehend the organization's operational context. Knowledge and skills in this area should cover aspects such as:
- Organization size, structure, functions and relationships,
- General business processes and related terminology, and
- Cultural and social customs of the auditee.

6.2.4 Applicable laws, regulations and other obligations: to enable the auditor to work within, and be aware of, various obligations towards information security, privacy, governance and other requirements that apply to the organization being audited. Knowledge and skills in this area should cover relevant:
- Local, regional and national codes, laws and regulations;
- Contracts and agreements;
- International treaties and conventions; and
- Other compliance requirements such as applicable standards.

6.3 Lead Auditors' Qualifications

6.3.1 Audit team leaders should have additional knowledge and skills in audit leadership to facilitate the efficient and effective conduct of the audit. An audit team leader should be able to:
- Plan the audit and make effective use of resources during the audit;
- Represent the audit team in communications with the audit client and auditee;
- Organize, direct and motive audit team members;
- Mentor and provide guidance to auditor team members;

- Lead the audit team to reach the audit conclusions;
- Prevent or resolve conflicts; and
- Prepare and complete the audit report.

6.4 Specific Knowledge and Skills of ISMS Auditors.

6.4.1 Information security management system auditors should have knowledge and skills in Information security-related methods and techniques. To enable the auditor to examine information security management systems and to generate appropriate audit findings and conclusions. Knowledge and skills in this area should cover
- Information security terminology and concepts;
- Information security management principles and their application; and
- Information security management tools and their application.

6.4.2 Processes and products, including services: to enable the auditor to comprehend the technological context in which the audit is being conducted. Knowledge and skills in this area should cover:
- Industry-specific terminology;
- Technical characteristics of processes and products, including services, and industry-specific processes and practices.

7 Records

7.1 As well as miscellaneous audit evidence (such as copies of documents, audit notes, records of interviews, system printouts *etc.*), ISMS internal audits generate the following formal records:
- Audit programme
- Audit plan/Notification
- Audit checklist/Observation sheet
- Systemic requirements checklist
- Control requirements checklist
- Internal audit Report
- Non-conformity/Corrective and Preventive Action report (NCPAR)

7.2 All information shall be appropriately secured given its often confidential nature.

7.3 All information shall be properly filed and indexed.

06.Information classification matrix

What exactly is meant by the term "ISO 27001 Information Classification"? [10] The process of determining how much security should be afforded to the information that an organization possesses is known as information classification. This process is carried out by the organization. Information is typically categorized in terms of its level of confidentiality by organizations.

Click here to view document

ISO 27001 security

INFORMATION CLASSIFICATION MATRIX AND HANDLING GUIDE

CATEGORY	DESCRIPTION	Sample Documents/Records	MARKING	PHYS & ADMIN CONTROLS	REPRODUCTION	DISTRIBUTION	DESTRUCTION/ DISPOSAL
PUBLIC or open	Information that may be broadly distributed without causing damage to the organization, its employees and stakeholders. The [PR Office/Marketing Dept/Information Security Management dept/etc.] must pre-approve the use of this classification. These documents may be disclosed or passed to persons outside the organization.	Marketing materials authorized for public release such as advertisements, brochures, published annual accounts, Internet Web pages, catalogues, external vacancy notices	None	None	Unlimited	No restrictions	Recycling/trash
INTERNAL or proprietary	Information whose unauthorized disclosure, particularly outside the organization, would be inappropriate and inconvenient. Disclosure to anyone outside of [Company name] requires management authorization.	Most corporate information falls into this category. Departmental memos, information on internal bulletin boards, training materials, policies, operating procedures, work instructions, guidelines, phone and email directories, marketing or promotional information (prior to authorized release), investment options. transaction data, productivity reports, disciplinary reports, contracts, Service Level Agreements, internal vacancy notices, intranet Web pages	"**INTERNAL USE ONLY**" Apply to bottom left corner of each page.	**Author:** responsible for proper markings. **User:** responsible for proper storage and document control.	Limited copies may be made only by employees, or by contractors and third parties who have signed an appropriate nondisclosure agreement.	**Internal**: use an internal mail envelope. **External**: use a sealed envelope. **Electronic**: use internal email system. Encryption is required for transmission to external email addresses. **FAXing**: take care over the FAX number!	**Paper documents:** shred. **Electronic data:** erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal
CONFIDENTIAL or restricted	Highly sensitive or valuable information, both proprietary and personal. Must not be disclosed outside of the organization without the explicit permission of a Director-level senior manager.	Passwords and PIN codes, VPN tokens, credit and debit card numbers, personal information (such as employee HR records, Social Security Numbers), most accounting data, other highly sensitive or valuable proprietary information	"**CONFIDENTIAL**" Apply to bottom left corner of each page.	**Originator:** responsible for ensuring that confidential information is distributed on a strict need-to-know basis. **Recipient:** responsible for ensuring that confidential information is encrypted and/or kept under lock & key when not in use	Limited copies may be made only by permission of originator or his/her designates. A signed authorization slip will be presented.	**Internal:** use a sealed envelop inside an internal mail envelope. Hand deliver if possible. **External:** use a plain sealed envelope. Hand deliver or send by registered mail, courier etc. **Electronic:** use internal email system only. Encyrpt data. **FAXing:** requires phone confirmation of receipt of a test page immediately prior to sending the FAX, and phone confirmation of full receipt.	**Paper documents:** shred using an approved cross-cut shredder. **Electronic data:** erase or degauss magnetic media. Send CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate disposal.

07.IS027k ISM organization chart data

Click here to view document

Name	Reports_to	Title	Department	Telephone
samantha		Chief Security Officer	Executive	x8845
theshi	samantha	Information Security Manager	ISM	x8856
kamila	theshi	Security Policies and Complianc	ISM	x8821
hemantha	kamila	Head of Security Administration	ISM	x8843
demantha	hemantha	Security Administrator	ISM	x8820
tushara	demantha	Security Administrator	ISM	x8860
chamitha	tushara	Security Risk and Contingency M	ISM	x8810
sathushka	chamitha	Local Security Committee	Various	x8870
yohara	sathushka	Local Security Committee	Various	x8855
rasanjana	yohara	Security Operations	ISM	x8853
hasintha	rasanjana	Security Architect	ISM	x8890
nanayakara	hasintha	Security Officer	ISM	x8811
lasantha	nanayakara	Information Asset Owner	Various	x8812
hasantha	lasantha	Information Asset Owner	Various	x8813
Asanka	samantha	Physical Security Manager	Physical Security	x8814
karunanayeke	Asanka	Security Guard	Physical Security	x8815

08.IS027k SOA 2013 English and Spanish updated

Your information security management system (ISMS) would be incomplete without the Statement of Applicability (SoA) (ISMS). [11]One of the most crucial papers you'll need to create for ISO 27001:2013 certification is the statement of applicability (SoA).The SoA simply specifies what ISO 27001 controls and policies are being used by the organization to secure valuable information assets and manage the information processing facilities. It is compared to ISO 27001's Annex A control set as a benchmark (described at the back of that ISO standards document as reference control objectives and controls).ISO 27001's applicability statement can be found in section 6.1.3 of the standard's major requirements. This section is part of section 6.1, which is concerned with taking steps to deal with threats and opportunities. Therefore, the SoA is an essential component of the ISO 27001 documentation that must be provided to an external

auditor during an independent audit of the ISMS, such as by a UKAS audit certification authority.

Click here to view document

Statement of Applicability

Current as of: 16/09/2022

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Annex A controls			Current controls	Remarks (with justification for exclusions)	Selected controls and reasons for selection				Remarks (overview of implementation)
Clause	Sec	Control Objective/Control			LR	CO	BR/BP	RRA	
5 Security Policies	5.1	Management direction for information security							
	5.1.1	Policies for information	*	Exiting System			*	*	Implemeny ACL
	5.1.2	Review of the policies for information security	*	SOC			*		
6 Organisation of information security	6.1	Internal organisation							
	6.1.1	Information security roles and responsibilities	*	Exiting System		*	*		
	6.1.2	Segregation of duties		Small Organization,No fund Allocated					Various Departments
	6.1.3	Contact with authorities		Small Organization,No fund Allocated					
	6.1.4	Contact with special interest groups		Small Organization,No fund Allocated					
	6.1.5	Information security in project management		Small Organization,No fund Allocated					
	6.2	Mobile devices and teleworking							
	6.2.1	Mobile device policy		Small Organization,So Controlable					
	6.2.2	Teleworking		Small Organization					
7 Human resource security	7.1	Prior to employment							
	7.1.1	Screening	*	Exiting Controls		*	*		Formal Interviews
	7.1.2	Terms and conditions of employment	*	Exiting Controls		*	*		Formal Interviews
	7.2	During employment							
	7.2.1	Management responsibilities	*	Exiting Controls		*	*		
	7.2.2	Information security awareness, education and		Exiting Controls		*	*		
	7.2.3	Disciplinary process		Not Considering as an issue					
	7.3	Termination and change of employment							
	7.3.1	Termination or change of employment		Not Considering as an issue					
8 Asset management	8.1	Responsibility for assets							
	8.1.1	Inventory of assets		Small Organization					
	8.1.2	Ownership of assets	*	Exiting Controls			*		
	8.1.3	Acceptable use of assets	*	Exiting Controls			*		Authenticate and Authorize Users
	8.1.4	Return of assets		Not returning Assets					
	8.2	Information classification							
	8.2.1	Classification of information		No large classification					
	8.2.2	Labeling of information		No large classification					
	8.2.3	Handling of assets	*	Exiting Controls			*		
	8.3	Media handling							
	8.3.1	Management of removable media		No media assests are implemented					
	8.3.2	Disposal of media		No media assests are implemented					
	8.3.3	Physical media transfer		No media assests are implemented					
	9.1	Business requirements of access control							
	9.1.1	Access control policy	*	Exiting Controls	*	*			Implement ACL and privilledges
	9.1.2	Access to networks and network services	*	Exiting Controls	*	*			
	9.2	User access management							

	8.3.3	Physical media transfer		No media assests are implemented					
9 Access control	9.1	Business requirements of access control							
	9.1.1	Access control policy	*	Exiting Controls	*	*			Implement ACL and privilledges
	9.1.2	Access to networks and network services	*	Exiting Controls	*	*			
	9.2	User access management							
	9.2.1	User registration and de-registration		Not frequently changing vacancies					
	9.2.2	User access provisioning							
	9.2.3	Management of privileged access rights		Not frequently changing vacancies					
	9.2.4	Management of secret authentication information of	*	Exiting Controls	*	*			
	9.2.5	Review of user access rights							
	9.2.6	Removal or adjustment of access rights		Not Considering as an issue					
	9.3	User responsibilities							
	9.3.1	Use of secret authentication information	*	Exiting Controls	*	*			
	9.4	System and application access control							
	9.4.1	Information access restriction							
	9.4.2	Secure log-on procedures							
	9.4.3	Password management system	*	Exiting Controls	*	*			Implement ACL and privilledges
	9.4.4	Use of privileged utility programs							
	9.4.5	Access control to program source code							
10 Cryptography	10.1	Cryptographic controls							
	10.1.1	Policy on the use of cryptographic controls		Exiting Controls					
	10.1.2	Key management		Exiting Controls					
11 Physical and environmental security	11.1	Secure areas							
	11.1.1	Physical security perimeter		Small Organization					
	11.1.2	Physical entry controls		Small Organization					
	11.1.3	Securing office, room and facilities		Small Organization					
	11.1.4	Protecting against external end environmental		Small Organization					
	11.1.5	Working in secure areas		Small Organization					
	11.1.6	Delivery and loading areas		Small Organization					
	11.2	Equipment							
	11.2.1	Equipment siting and protection		Small Organization					
	11.2.2	Supporting utilities		Small Organization					
	11.2.3	Cabling security		Small Organization					
	11.2.4	Equipment maintenance		Small Organization					
	11.2.5	Removal of assets		Small Organization					
	11.2.6	Security of equipment and assets off-premises		Small Organization					
	11.2.7	Secure disposal or re-use of equipment		Small Organization					
	11.2.8	Unattended user equipment		Small Organization					
	11.2.9	Clear desk and clear screen policy		Small Organization					
	12.1	Operational procedures and responsibilities							
	12.1.1	Documented operating procedures		Not Considering as an issue					
	12.1.2	Change management		Not Considering as an issue					
	12.1.3	Capacity management		Not Considering as an issue					
	12.1.4	Separation of development, testing and operational environments		Not Considering as an issue					
	12.2	Protection from malware							

	12.1	Operational procedures and responsibilities							
	12.1.1	Documented operating procedures		Not Considering as an issue					
	12.1.2	Change management		Not Considering as an issue					
	12.1.3	Capacity management		Not Considering as an issue					
	12.1.4	Separation of development, testing and operational environments		Not Considering as an issue					
	12.2	Protection from malware							
	12.2.1	Controls against malware		exiting Controls					
	12.3	Backup							
	12.3.1	Information backup		exiting Controls					
12 Operations security	12.4	Logging and monitoring							
	12.4.1	Event logging		Small Organization					
	12.4.2	Protection of log information		Small Organization					
	12.4.3	Administrator and operator logs		Small Organization					
	12.4.4	Clock synchronisaton		Small Organization					
	12.5	Control of operational software							
	12.5.1	Installation of software on operational systems		Exiting Controls	*	*			Server is running on linux and compu
	12.6	Technical vulnerability management							
	12.6.1	Management of technical vulnerabilities		Small Organization					
	12.6.2	Restrictions on software installation		Small Organization					
	12.7	Information systems audit considerations							
	12.7.1	Information systems audit controls		Small Organization					
	13.1	Network security management							
	13.1.1	Network controls		Small Organization					
	13.1.2	Security of network services		Small Organization					
13 Communications security	13.1.3	Segregation in networks		Small Organization					
	13.2	Information transfer							
	13.2.1	Information transfer policies and procedures		Small Organization					
	13.2.2	Agreements on information transfer		Small Organization					
	13.2.3	Electronic messaging		Small Organization					
	13.2.4	Confidentiality or non-disclosure agreements		Small Organization					
	14.1	Security requirements of information systems							
	14.1.1	specification		Exiting Controls	*	*			
	14.1.2	Securing applications services on public networks		Exiting Controls	*				
	14.1.3	Protecting application services transactions		Exiting Controls			*		
	14.2	Security in development and support processes							
	14.2.1	Secure development policy		Not Developing Softwares					
	14.2.2	System change control procedures		Not Developing Softwares					
14 System acquisition, development and maintenance	14.2.3	Technical review of applications after operating platform changes		Not Developing Softwares					
	14.2.4	Restrictions on changes to software packages		Not Developing Softwares					
	14.2.5	Secure system engineering principles		Not Developing Softwares					
	14.2.6	Secure development environment		Not Developing Softwares					
	14.2.7	Outsourced development		Not Developing Softwares					
	14.2.8	System security testing		Not Developing Softwares					
	14.2.9	System acceptance testing		Not Developing Softwares					
	14.3	Test data							
	14.3.1	Protection of test data		Not Developing Softwares					
	15.1	Information security in supplier relationships							
	15.1.1	Information security policy for supplier relationships		Not Considering as an issue					
	15.1.2	Addressing security within supplier agreements		Not Considering as an issue					
15 Supplier relationships	15.1.3	Information and communication technology supply		Not Considering as an issue					
	15.2	Supplier service delivery management							
	15.2.1	Monitoring and review of supplier services		Not Considering as an issue					
	15.2.2	Managing changes to supplier services		Not Considering as an issue					
	16.1	Management of information security incidents and improvements							
	16.1.1	Responsibilities and procedures		Small Organization					
	16.1.2	Reporting information security events		Small Organization					
16 Information security incident management	16.1.3	Reporting information security weaknesses		Small Organization					
	16.1.4	Assessment of and decision on information security		Small Organization					
	16.1.5	Response to information security incidents		Small Organization					
	16.1.6	Learning from information security incidents		Small Organization					
	16.1.7	Collection of evidence		Small Organization					
	17.1	Information security continuity							
	17.1.1	Planning information security continuity		Exiting Controls	*				
	17.1.2	Implementing information security continuity		Exiting Controls		*	*		
17 Information security aspects of business continuity management	17.1.3	Verify, review and evaluate information security		Exiting Controls	*		*		
	17.2	Redundancies							
	17.2.1	Availability of information processing facilities		Not Considering as an issue					
	18.1	Compliance with legal and contractual requirements							
	18.1.1	Identification of applicable legislation and contractual requirements		Not Considering as an issue					
	18.1.2	Intellectual property rights		Not Considering as an issue					
	18.1.3	Protection of records		Not Considering as an issue					
18 Compliance	18.1.4	information		Not Considering as an issue					
	18.1.5	Regulation of cryptographic controls		Not Considering as an issue					
	18.2	Information security reviews							
	18.2.1	Independent review of information security		Not Considering as an issue					
	18.2.2	Compliance with security policies and standards		Not Considering as an issue					
	18.2.3	Technical compliance review		Not Considering as an issue					

09.Nonconformity corrective preventive action form

It's possible that failing to meet an ISMS obligation constitutes nonconformity. [12]Since human error is inevitable in any organization, preventing nonconformity is unrealistic. What is crucial, however, is that the problem be recognized and addressed appropriately whenever it arises. Statements, inferences, or obligations all qualify as requirements.

Click here to view document

ISO 27001 security

NCPAR № NC-42-882	**Non-conformity/Corrective & Preventive Action Report (NCPAR)**	Date NC Found: 18th September 2022
Department or Section where NC is found:		

1. DETAILS: Nonconformity raised as a result of:

☐ Internal audit ☐ Customer complaint ☐ IS Incident, indicate IS number: _____
☐ Process non-conformity ☐ Suggestion (improvement)
☐ Product non-conformity ☐ Others _____

2. REFERENCES: Documents used or referred-to (e.g. manuals, procedures, flowcharts, standards, records …)

Audit Report
Security Procedures Manual

3. NON-CONFORMITY: Description of nonconformity, suggestion, complaint or incident.

Detected or Observed by: CEO	Department: Admin

4. DISPOSITION: Immediate remedial action

Proposed by:	Date:	Implementation date:

5. INVESTIGATION: Cause of nonconformity: (investigation shall be conducted by the department or section where the nonconformity was found)

Investigated by:	Date investigation started:
	Date investigation finished:

ISO 27001 security

6. CORRECTIVE/PREVENTIVE ACTION: (Preventive action is only required for potential non-conformities). Fill ONLY EITHER "Corrective Action" OR "Preventive Action"

Corrective Action:	Preventive Action:
Proposed by:	Date:
	Proposed implementation date:

7. VERIFICATION OF VALIDITY OF CORRECTIVE "or" PREVENTIVE ACTION:

☐ Addresses the root cause? ☐ Prevents recurrence? ☐ Valid ☐ Invalid. Issue new NCPAR Remarks: _____	☐ Addresses the root cause? ☐ Prevents occurrence? ☐ Valid ☐ Invalid. Issue new NCPAR Remarks: _____
Signature: (Lead Auditor) / Date:	Signature: (Lead Auditor) / Date:

8. FOLLOW-UP OF IMLEMENTATION CORRECTIVE/PREVENTIVE ACTION TAKEN:

Implementation of corrective action is: ☐ Implemented ☐ Not implemented. Issue new NCPAR Remarks: _____	Implementation of preventive action is: ☐ Implemented ☐ Not implemented. Issue new NCPAR Remarks: _____
Signature: (Lead Auditor) / Date:	Signature: (Lead Auditor) / Date:

9. VERIFICATION OF EFFECTIVENESS OF IMPLEMENTED CORRECTIVE/PREVENTIVE ACTION:

10.Risk Assessment

Clause 6.1.2, "Information Risk Assessment," is a mandatory section of the ISO 27001 standard. Information security risk assessment processes, including risk acceptance and assessment criteria, must be established and maintained as per this clause. [13]The assessments must also be consistent, valid, and yield "similar resources," as required (clearly describing the approach being taken).In order to determine what threats there are to the CIA (confidentiality, integrity, and availability) of information assets within the ISMS's purview, organizations must apply these assessment techniques. The risks must then be delegated to risk owners within the organization, who must independently evaluate each risk's severity, weigh the potential fallout from its realization, and settle on the risk's "probability" of materializing. After this threat has been assessed, it must be dealt with using the methods outlined in the risk management strategy.

Click here to view document

Information Assest	Known or suspected Threats	Known or suspected Vulnerabilities	Primary Concerns (C | I | A)	Probability or Occurance	Impact Level	Raw Risk Level	Secuirty Controls	Incident Undetectibility	Detected Risk Level	Risk Total
Servers	Theft Attack	Physcially easy access to the site	A	1	4	4	Access Control Policies, Lock doors, Physcial Security	1	4	7
	Accidental or criminal damage, sabotage	HVAC control	A+I	1	4	4	Best practices, Data protection policies	1	4	
	Hacking	Internet Connectivity and 3rd party connectivity to outside Networks	C+I	2	4	8	Firewall, IDS, IPS,Patch Updates	4	24	
	Fire, flood	Redundant servers	A	1	4	4	Physical security, Countengency plan	1	4	
Billing Database	Hacking	internet connectivity, lesser firewall protection	C+I	1	4	4	Data protection policies & procedures; network security controls; system security controls	3	12	10
	Poor quality data	Poor quality information	A+I	1	2	2	Built in Integrity Properties	3	8	
	Virus and other Malware	SQL attacks and Sniffers	C+I	1	4	4	Data protection policies & procedures; ongoing awareness program	4	16	
Desktop/Laptops used by the Employee	Theft Attack	Physcially easy access to the site	A	4	3	12	CCTV, Swipe Cards, Lock Doors	1	12	17
	Virus and other Malware	USB Drives and Internet Connectivity	C+I	4	3	12	Increase of user awareness and Use of updated virus guards	2	24	
	Accidental or criminal damage, sabotage	HVAC control	A+I	1	3	3	Policies with best practices	1	3	

Desktop/Laptops used by the Employee										17
	Virus and other Malware	USB Drives and Internet Connectivity	C+I	4	3	12	Increase of user awareness and Use of updated virus guards	2	24	
	Accidental or criminal damage, sabotage	HVAC control	A+I	1	3	3	Policies with best practices	1	3	
Website	Hacking	Internet connectivity	I+A	2	3	6	Network security controls and implementing a DMZ	3	18	15
	Network Attack	DOS, SQL attacks	A+I	1	3	3	Firewall	1	3	
	Social engineering	Lack of policies	C	1	3	3	Policies with best practices	4	12	
	Virus and other malware	internet Connectivity and Sniffers	C	3	3	9	Virus guard, NMS tools	5	45	16
LAN	Data or system corruption	Packet Drops	A	2	2	4	Data Protection, Network Security policies	3	12	
	Physcial Damage	Cable Destruction	A	1	2	2	Proper physcial structure standards	3	6	
	Theft	Physcially easy access to the site	C	2	4	8	Physical Access Control Policies	2	16	5.3
Backup Drive	Accidental or criminal damage, sabotage	Poor standars for storing	I+A	2	3	6	Best practices, Data protection policies	1	6	
	Fire, flood	No fire, alarm	A	0	5	0	Physical security, Countengency plan	2	0	

Conclusion

RedArms security company is covering the all island wide security measures and its provide as the security of database, network and firewall in to the organizations and top leading companies. This report delves deep into what ISO27001 Audit Controls are and how they can improve the company's Cyber Security. The ISO 27001 standard is deeply ingrained in the company's culture. Organizations can better adapt to evolving information security threats by adhering to this standard. A company's vulnerability to cyberattacks and data breaches can be greatly mitigated through an information security management system. RedArms Security Company should implement the standards for very critical departments and services with the cost analysis. This stage defines the scope of your ISMS and its daily impact. If your scope is too small, you risk your organization's security. Too much scope will make the ISMS difficult to manage. This can give protection to the organization and system information to implement some security policy as well as the security step. In some ways, this cloud be extremely beneficial to the organization in the future.

References

[1] "5 steps to an effective ISO 27001 risk assessment," [Online]. Available: https://www.itgovernance.eu/blog/en/what-is-an-iso-27001-risk-assessment-and-how-should-you-report-on-it#:~:text=An%20ISO%2027001%20risk%20assessment,in%20their%20information%20security%20processes..

[2] 7. S. t. a. S. I. 2. R. Assessment. [Online]. Available: https://www.itgovernance.co.uk/blog/7-steps-to-a-successful-iso-27001-risk-assessment.

[3] "ISO/IEC 27001," [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html.

[4] "5 benefits of ISO 27001 certification," [Online]. Available: https://www.itgovernance.eu/blog/en/benefits-of-iso-27001-certification.

[5] "What is an ISMS (Information Security Management System)?," [Online]. Available: https://www.itgovernanceusa.com/blog/what-exactly-is-an-information-security-management-system-isms-2.

[6] "What is an Internal Audit? Answers to Common Questions," [Online]. Available: https://linfordco.com/blog/what-is-internal-audit/.

[7] "How to build the business case for your ISMS," [Online]. Available: https://www.isms.online/isms-business-case-builder/building-the-case-for-an-isms/.

[8] "ISO27k Model Policy On Change Management and Control," [Online]. Available: https://www.scribd.com/document/285615448/ISO27k-Model-Policy-on-Change-Management-and-Control.

[9] [Online]. Available: https://www.isms.online/iso-27001/what-is-the-iso-27001-audit-process/.

[10] "What is ISO 27001 Information Classification?," [Online]. Available: https://www.itgovernance.co.uk/blog/what-is-information-classification-and-how-is-it-relevant-to-iso-27001.

[11] "ISO 27001:2013 Statement of Applicability (SoA): The Complete Guide," [Online]. Available: https://www.isms.online/iso-27001/iso27001-statement-applicability-simplified/.

[12] "ISO 27001 Clause 10.1 Non conformity and corrective action," [Online]. Available: https://info-savvy.com/iso-27001-clause-10-1-non-conformity-and-corrective-action/.

[13] "ISO 27001 Risk Assessment," [Online]. Available: https://www.isms.online/iso-27001/risk-assessment/.