K.P.I. Shenesh Perera

IDM Negombo | ISMS

Information Security Management System

Garkeen supermarket

**Contents**

[Information Security Management System 3](#_Toc12306925)

[Briefing 3](#_Toc12306926)

[Defining the Information Security Management System 3](#_Toc12306927)

[What is an ISMS? 3](#_Toc12306928)

[What are the principles of an ISMS? 4](#_Toc12306929)

[Why an ISMS? (Advantages of an ISMS) 4](#_Toc12306930)

[Compliance Statement to ISO:27001:2013 5](#_Toc12306931)

[Planning (Clause 4 & 5) 6](#_Toc12306932)

[Risk Assessment 6](#_Toc12306933)

[Security Policy 8](#_Toc12306934)

[General security 8](#_Toc12306935)

[Password eligibility and maintenance 8](#_Toc12306936)

[Virus and malware 9](#_Toc12306937)

[Firewalls, VPNs, Load-balancers and procedures taken to prevent commonly known exploits. 10](#_Toc12306938)

[Backups and fallback procedures 10](#_Toc12306939)

[Implementation (Clause 6 & 7) 12](#_Toc12306940)

[Implementation Compliance to ISO:27001:2013 12](#_Toc12306941)

[Security teams & system access control 12](#_Toc12306942)

[Awareness, training programs and consequences of disobedience to the Garkeens Supermarket 14](#_Toc12306943)

[Commitment 15](#_Toc12306944)

[How does ISO:27001:2013 support the ISMS? 15](#_Toc12306945)

[Monitoring (Clause 8 & 9) 16](#_Toc12306946)

[Tools and procedures that will assist in monitoring 16](#_Toc12306947)

[Auditing (External or Internal) 16](#_Toc12306948)

[Various software that can be used to monitor the system 17](#_Toc12306949)

[Improvements (Clause 9) 18](#_Toc12306950)

[How does ISO align with the controls and procedures used for monitoring and improvement? 18](#_Toc12306951)

[Advantages and disadvantages of ISO:27001:2013 19](#_Toc12306952)

[ISO:27001 vs other security standards 20](#_Toc12306953)

# Information Security Management System

## Briefing

This information security management system design document will consist of the core components enlisted by ISO:27001:2013 framework, through design to implementation then to monitoring assurances, this document will consist of extremely valuable information to the company.

**This document is the blueprint for all security movements taken place within Garkeens, as such the highest priority is to protect this document.** The necessary precautions to keep this document from falling into the wrong hands will also promptly be discussed.

Per the ISO:27001:2013 framework description, in order for this document to be of expected standard, the document will cover the following components in deep details:

* Risk assessment and grading through a risk assessment matrix
* Documented controls and processes
* Security awareness, guidance, training and competencies
* Tools, technology and equipment that will contribute to the protection, security and monitoring that all protocols dictated within this document are followed

# Defining the Information Security Management System

## What is an ISMS?

It is a centrally managed framework in order to keep the sensitive or non-sensitive information (judged and assumed as to the sensitivity by the framework) safe and available. It dictates a set of policies, procedures and physical controls that allow to maintain the 3 principles of information security.

An ISMS does not only include technical controls but also spreads its influence to people, resources, assets and processes. This is done through a risk assessment in an organization that considers both internal and external risks to an organization. All risks will be assessed, analyzed and evaluated against a predefined criteria before security protocols are applied. The predefined criteria classifies risks and vulnerabilities on the degree of an impact and the potential of a risk.

By doing so, an ISMS aims to allow an organization to make appropriate decisions about the risks that are unique to the organization’s IT economy, and as such an ISMS documented for one organization cannot be used for another organization.

With all these facts it is possible to say that defining an ISMS is not an IT function it is a business management process.

A good, valid and pragmatic ISMS can be certified by the international best-practice information security standard known as the ISO:27001. Achieving this certification, demonstrates that the organization’s security protocols are of a standard. This standard is a badge of trust for customers, regulators, stakeholders and any external party that may consider to partake within the organization as ISO:27001 standardization boasts the best practices to secure an organization’s information.

## What are the principles of an ISMS?

The principles for an ISMS are the same that of information security, an ISMS is designed, implemented and monitored to ensure the unanimous flow of the following three golden principles:

1. Confidentiality – To provide access to only the authorized personnel who by the ISMS are assumed and dictated to be eligible for access to the organization’s system
2. Integrity – Keeping the validity, accuracy and the completeness of the information of the organization through carefully outlined enforcement of precautionary rules.
3. Availability – Ensuring that the information is available to a user that is eligible for authorization (as per dictated by the ISMS) when they require it.

## Why an ISMS? (Advantages of an ISMS)

The advantages of implementing an ISMS are as follows and will be presented in bullet-form:

* Secures your information in every way and form – Data is protected locally and on any external storages
* Increases your protection against cyberattacks – Maintaining an ISMS will significantly boost your protection levels against cyberattacks.
* Response/Reactivity to cyberattacks or any factor that may attempt to damage the organization is much higher – If some factor comes to place and occurs, then Garkeen Supermarket can respond to this problem, which is something thus far it has been incapable of doing.
* Employees will be aware and responsible – Through the training procedures and various orientations that will occur, employees in Garkeen are less likely to use company resources in ways that will endanger the security of the organization’s important assets.
* Reduces costs associated with securing information – Through risk assessment matrices that are documented, Garkeen will not have to spend time on putting together or thinking of unnecessary and possibly outdated solutions to threats, that are not cost effective.
* Maintains the core principles of information security – Confidentiality, Integrity and Availability will be thoroughly maintained through the use of an ISMS.
* Gives sense of safety and confirmation to customers – Through ISO:27001 certifications and the protocols of an ISMS, customers will be able to see Garkeen Supermarket in a new window of light and will allow the company to regain lost trust and reputation.

## Compliance Statement to ISO:27001:2013

**The Information Security Management System that is henceforth dictated in this document has been designed per the ISO:27001:2013 framework.**

**The implementation of the ISMS will grant users of this document to safely and properly retrieve and store information. This ISMS composes of policies, standards, procedures, practices, behaviors and activities that will help and only help Garkeens Supermarket to protect its information.**

**All needs and objectives of the organization has been taken into count and will be addressed throughout the document. The purpose of this document is to identify, assess and manage risks or vulnerabilities to the information within the organization.**

**As per the legislation of the ISO:27001:2013 framework, the structure of the ISMS will be as follows:**

* **Clause 4: Design**
* **Clause 5: Design**
* **Clause 6: Implement**
* **Clause 7: Implement/Operate**
* **Clause 8: Operate**
* **Clause 9: Monitor/Improve**
* **Clause 10: Improve**

**Any who reads this document, hereby adheres to following this document word by word, without question, doubt or modification to what’s dictated.**

**Any who intentionally goes against what is dictated within this document will face appropriate consequences and is guilty so will immediately be charged for violation of the ISMS.**

**Any who claims unintentional violation will be tested, interrogated and questioned.**

**Innocence MUST be granted UNTIL proven guilty.**

# Planning (Clause 4 & 5)

In this clause, the document will aim to cover two key components of the Information Security Management System:

* Address risks and vulnerabilities
* Address information security objectives

This clause attempts to cover these two key components by assessing risks and then treating them through the putting forth a security policy. The first part of the clause therefore attempts the declare the requirement to see that events that have already occurred do not re-occur, through suitable improvement to processes and workflow. These improvements are not limited to preventing situations that have already occurred, but also those that could happen.

## Risk Assessment

In the risk assessment procedure, the document will attempt to grade each risk through the following formula:

The fact that a threat may occur is a risk, where Impact is the damage, effect or consequences of a threat occurring, and potential is the likelihood of this particular threat occurring. Both Impact and Potential will have the minimum of 0 and maximum of 5, with 0 being trivial and 5 being extremely dangerous. Trivial risks will be noted but not accounted for. This formula will be used to graduate each risk in the risk assessment matrix below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Impact** | **Potential** | **Grade** | **Evaluation** |
| Damage caused by malware and harmful software | 2 | 4 | 3 | The grade depends on how complex and damaging the virus is, this grade is an average. |
| Management Information System Data leaks | 5 | 3 | 4 | Leaks of MIS have been confirmed and this was done by a rookie company. Action required. |
| Mailing server exploitation | 5 | 2 | 3.5 | Recent mail campaigns were not able to be carried out, for nearly 2 months. Action required. |
| Lack of basic security devices like firewalls and VPNs which could lead to mass exploitation | 5 | 4 | 4.5 | This is one of the primary reasons why Garkeens is vulnerable. Action **must** be taken. |
| Unavailablity due to lack of backup servers | 5 | 4 | 4.5 | Systems fail for far too long, this is a direct cut in the profits of the company. Action **must** be taken. |
| Lack of backup schedule for databases leading to loss of data | 3 | 1 | 2 | No backups means no data restoring, if by chance data is lost there is no way to recover |
| Unintentional data corruption | 2 | 3 | 2.5 | Through badly written SQL statements or improperly done implementations |
| Lack of copyrights to claim authority of information | 5 | 4 | 4.5 | When customer data was stolen recently Garkeens was unable to respond properly. Action **must** be taken |
| (Distributed) Denial of Service attacks | 4 | 2 | 3 | Will effectively deny the service to clients and users of the system, action required. |
| Cross-Site Reference Attacks | 3 | 2 | 2.5 | Through improperly sanitized HTML entities or usage of innerHTML for DOM manipulation, will give attacker complete authority over web server. |
| SQL Injection | 4 | 3 | 3.5 | Highly probable method of attack as to how the customr and MIS data was stolen |
| System unavailability through power cuts | 3 | 5 | 4 | Highly probable in Sri Lanka, due to regular powercuts systems maybe unavailable. Action **must** be taken |
| Lack of proxies to disable employees from using internet to surf irresponsibly | 1 | 5 | 3 | This could expose the system for unwanted attacks through the internet. Action required |
| Lack of backup devices in case of system failure | 3 | 1 | 2 | In case of system failure, there must be systems ready to replace the failed system. |

## Security Policy

### General security

Garkeens Supermarket and its responsible staff handle data and information of various grades of sensitivity. Sensitive Information must have adequate safeguards in place to protect them, to protect customer privacy, to ensure compliance with ISO:27001:2013 and to guard the future reputation, trust customers have and the efficiency of the organization.

Upon the creation of this document, Garkeens Supermarket hereby promises to commit to respecting the privacy of all its customers and to protect any and all data about customers from external entities.

To this end the management, IT staff and every other employee that directly interacts with any system that collects, stores or reads data must read this policy **before being deployed to the workforce.** The security policy at a glance ensures to:

* Handle company and customer information in a manner that fits their sensitivity.
* Limit personal use of Garkeens Supermarket information and telecommunication systems and ensure it doesn’t interfere with employee job performance
* **Only Garkeens AUTHORIZED staff** reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for **AUTHORIZED** purposes.
* Not use company e-mail addresses, internet or any other company resource to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal.
* Not disclose personnel information unless authorized, if you belong to department that handles the economy, accounts or decisions that will directly affect Garkeens Supermarket.
* Keep passwords and accounts secure.
* Request approval from management prior to establishing any new software or hardware, third party connections, etc.
* Do not install unauthorized software or hardware specially flash drives, external hard disks, dongles, USB cables, remote access points, modems or any other electrical device that may in any way have access to the data in a device.
* Always leave desks clear of files, receipts or any documents that may contain, reflect or suggest sensitive data and lock computer screens when unattended.

### Password eligibility and maintenance

Every user that goes through authorization portals or any portal in the system controlled by Garkeens Supermarket that grants a certain level of access, must read this category.

Herein, all passwords stored in a database must be salted, hashed and encrypted before storing, in the case of a usage of key-based encryption, the key must be stored securely, and all decryption utilities must be thoroughly checked and tested for vulnerabilities whenever a new path, version update or an upgrade is done.

* All passwords must be atleast of 10 characters in length.
* By default, all systems that grant access through password entry must maintain the default standard of 1 upper and 1 lower alphabetical character and atleast 3 numerical values.
* Symbols like @, %, =, \_, (, ) etc. must not be allowed. Consecutive numerical values must be banned example: 123, 23, 45, 95.
* Passwords must not contain parts of the username.
* Passwords must be renewed every month, whenever a breach has taken place or if a new security policy law that rewrites password eligibility.
* All passwords of terminated, fired or resigned users must be immediately removed, alongside the user account. It is recommended to this **before** removing the employee from the company.
* While entering passwords to the system, no employee of any department level is eligible to screen-snooping unless the password is shown to be failing.
* Use industry level acceptable encryption algorithms like AES256 for encryption.

### Virus and malware

Software used to counter viruses and malware must be tested and researched thoroughly before usage. Per ISO:27001:2013, every action taken to eliminate viruses, malwares or any software based issue must be logged, reported to the responsible parties and be stored away in case a similar situation takes place again.

* The software that is used to counter viruses, malware and any malicious software must be capable of handling a multiple types of software threats and must be industrially accepted.
* All removable media like flash drives, hard drives etc. should be scanned for viruses **before** being used.
* All removal of malicious entities must be logged and handled as mentioned in the ISO:27001:2013.
* All the logs generated from the antivirus solutions have to be retained as per legal requirements of ISO:27001:2013 and suggested by this policy for at least 3 centrally online accessible and 1 year offline.
* The Antivirus software in use must be setup for automatic updates and periodic scans.
* Employees that are not responsible for maintaining the software must not be allowed to access the settings of the antivirus software.
* E-mails with attachments coming from suspicious or unknown sources should not be opened and must be immediately deleted. No one should forward any e-mail, which they suspect may contain virus.

### Firewalls, VPNs, Load-balancers and procedures taken to prevent commonly known exploits.

In compliance of ISO:27001:2013, firewalls, VPNs, routers, modems, load balancers and devices that are commonly used to ensure the effective performance and security of a system, must be used in the company. This part of the policy declares the eligibility, maintenance and what describes the best choice.

* All firewalls must be configured with in and outbound rules, and must not allow any external device to interact with the system.
* VPNs must be appropriately introduced to the system when anonymity and encrypted traffic are a significant provider. If an external VPN provider is used, per ISO:27001:2013, it must be industrially accepted and must have a solid past of customer satisfaction.
* All routers, modems, switches or any networking device that will be used for the purpose of maintaining, shaping and throttling traffic must come with documentation for installation, maintenance and to troubleshoot common known problems and must be industrially accepted, verified and made for industrial purposes.
* Load-balancers must be used in order to ensure optimal performance in delivering static and dynamic content. Additionally, all load balancers must be configured to have rate limits, so that they do not provide content repeatedly to the same endpoint which would result in slowing the network.
* Services like Cloudflare that promises to deliver anti-DDoS and any modern advanced flooding techniques that prevents the system from shutting down unexpectedly, must be implemented.
* All above security procedures must be applied to mailing servers.
* Traffic isolation must be done through the configuration of VLANs. Per the separation of concerns principle, any department, device or data flow within the system must be isolated in such a way that they do not affect any superior or inferior departments, devices or data flows.

### Backups and fallback procedures

In an event of unexpected data loss, corruption or unintentional overwrites, responsible employees must read this category and follow it’s every declaration.

* Every system that holds data that is significant and is sensitive must be backed up and stored safely everyday. Every week, the backups must be compressed and duplicated and stored in a main centralized storage and a local decentralized storage.
* Only employees that are responsible for backups are allowed to view backups.
* All backups must be readonly, there must be no tampering of data at any level.
* In the event of restoring a backup, an immediate maintenance phase must begin. No endpoint must be capable of accessing the system. During this phase, all efforts must be directed 24/7 to restoring the system to a functional state.
* Before installing a device or software, the data that is stored or read by the component that the device or software is being installed on must be backed up. Immediate fallback must take place if the device or software has been installed improperly, however the initial step must be to uninstall the installed device or software before restoring the backup.
* Backups that are over 6 working months, maybe disposed. The decision to whether or not it is disposed must be taken by the management.

# Implementation (Clause 6 & 7)

The implementation phase will be described as per ISO:27001:2013, it involves bringing awareness to employees of the system and conducting the necessary training sessions in order to ensure that the Garkeens Supermarket staff are aware of the Information Security Management System.

## Implementation Compliance to ISO:27001:2013

**The Information Security Management System Implementation phase that is henceforth dictated in this document has been designed per the ISO:27001:2013 framework.**

**The implementation of the ISMS will grant users of this document to safely and properly retrieve and store information. The implementation phase will assign the parties responsible for carrying out tasks and also ensure that Garkeens Supermarket Employees are aware and competent of what is within this document.**

**This part of the document must be read, understood and must be referred to by all employees in times of doubt.**

## Security teams & system access control

Per ISO:27001:2013, a security team responsible for ensuring the procedures of the ISMS are done and done correctly must be put into place. The following is the hierarchy of the suggested overview of what the security team must look like:

The above hierarchy does not reflect the hierarchy of power, authority and importance when it comes to the business, it is the direct reflection of who holds the least responsibility to the most responsibility when it comes to ensuring the practice of the ISMS.

The description and the roles of each member in the hierarchy are:

* Senior – The senior member has the highest level of access, and has the highest responsibility when it comes to ensuring the security of the information system that is in Garkeens Supermarket. The roles of this member are
  + Ensuring fellow members practice the ISMS and explaining when in doubt.
  + Must make necessary modifications to the ISMS depending on the state and the situation of the company.
  + Is indirectly responsible for any and all actions that result in data breaches, losses or corruptions.
  + Must make the necessary procedures with the management in order to ensure that the Garkeens Supermarket staff are trained and are well aware of the ISMS.
* Assistant Senior – The assistant senior member also has the highest level of access. The assistant must ensure that the flow of the hierarchy is in perform sync. Every action that is proposed by lower members must be presented to the assistant. The assistant will asses them and present it to the senior. The roles of this member are:
  + Supporting the Senior professionally with coming to conclusions or making decisions.
  + Ensuring that the hierarchy is in perfect flow.
  + Must process all documents that have to do with the security of Garkeens supermarket, before presenting to the Senior.
  + Must assist the Senior in making the necessary procedures with the management in order to ensure that Garkeens Supermarket staff are trained and are well aware of the ISMS.
  + Must ensure that the Senior lives upto the standards of those in the lowest of the hierarchy.
* Dept. Head – This member does not have to be the head of the department, but from each department, a Security based department head must be assigned. This member and the representatives of all the employees of that department during meetings. The roles of this member are:
  + Acting as a mediator between employees and the assistant senior security head.
  + Must attend all meetings that are related to new measures in the security or updates on the ISMS.
  + Must ensure that employees are following the ISMS to the standards.
* Employees – This member does not have any say, authority or power in the hierarchy. The sole responsibility of this member is to follow the commands of all those higher up in the hierarchy and also the protocols dictated in the ISMS document. The punishments faced by employees that do not ensure that they perform responsibly within the Garkeens Supermarket are documented below. Both parties that have committed, helped or purposely did not bring the department head are punished with the same punishment.

## Awareness, training programs and consequences of disobedience to the Garkeens Supermarket

The core of the implementation process is that the employees of Garkeens Supermarket follow the ISMS that has been documented. For the security of the supermarket to be influenced or improved to any degree, the components that make up most of the system and the ones that are most responsible of breaches and issues when it comes to security are the users of the system or the employees of Garkeens Supermarket.

Garkeens supermarket must set aside a monthly budget to ensuring that orientations, awareness and training programs are done in order to ensure that the employees are not only just following the ISMS but also to help clear doubts or issues that may otherwise make their work environment hostile.

These programs must be used as a way of collecting statistics and opinions of the ISMS in order to produce a healthy work environment, after all the worst enemy you could have are the employees. As such, the Senior security head is tasked with analyzing these statistics to optimize the ISMS in such a way that security is not compromised and it caters towards the large employee bases of Garkeens Supermarket.

All awareness, training and orientation programs must meet the following standards:

* All participants must be given a guidebook or an appealing leaflet that summarizes the program’s descriptions and explanations.
* The assistant and senior security heads must have given authorization and a green signal to performing the program.
* No external entities that do not partake in the consumption of company resources are allowed to participate in the program. Who attends and who doesn’t attend is entirely in the hands of the Senior security head.
* All programs awareness, training or orientation must either be held before work or after work with the compliance of the employees who will participate in the program.
* Following the programs, cutting boards, advertisements and banners must be placed all throughout the company where employees of Garkeens Supermarket spend most of their time at in order to ensure that they remember what they’ve learnt.
* If an employee is not capable of attending, the employee must provide a significant reason as to why not and then be directed to the department head, who will summarize the program’s contents.
* If an employee purposely/intentionally does not attend, they will be warned. Upon the 3rd **consecutive** warning, the senior head is to notify the management and an appropriate decision has to be made.
* If an employee has been caught violating the dictations and protocols of the ISMS document unintentionally, the employee will be excused but necessary actions must be taken by the security department head of that department in order to ensure that action does not repeat.
* If an employee has been caught violating the dictations and protocols of the ISMS document intentionally, the employee will be immediately charged. All actions done by the employee will be logged, then the employee will be interrogated and appropriately punished. Depending on the complexity and the significance of the action that the employee has taken, the management may or may not result to law suits. Permanent suspension from Garkeens Supermarket is also eligible in situations like this.

## Commitment

Any and all employee of Garkeen Supermarket must read out loud and pledge to the following in the beginning of every program:

**I hereby adhere to follow all principles, doctrines and protocols listed within this document and fully commit to following them. I will behave professionally and carry out my purpose as a member of the workforce of Garkeens Supermarket to the highest and most loyal degrees. I will never betray my fellow colleagues or my superiors or do any harm to the system that has been put to place by Garkeens Supermarket. I will provide the highest gratification and satisfaction to all customers of Garkeens Supermarket.**

**I stand witness to the, Information Security Management System authored by K.P.I. Shenesh Perera for Garkeens Supermarket that is in compliance of the International Standard Organization:27001:2013 security framework.**

## How does ISO:27001:2013 support the ISMS?

The ISO:27001:2013 framework assists greatly in putting forth the structure of the document in place. In order for declared ISMS to follow the ISO:27001:2013 framework the following must have been documented:

* Programs that will bring awareness and training to employees.
* Necessary security teams must be put into place.
* Responsible bodies must be identified.
* The responsibilities of each body must be outlined.
* Commitment
* All methods declared must be reasonable and within the limits of being logical enough to be implemented.
* Have the necessary explanation in order to ensure that all employees of an organization understands the ISMS (Does not use any technical wording that results in confusion).

All these principles have been taken note as the brain and heart of the ISMS documentation. The evidence to this claim are the wording above and below this statement. The ISO:27001:2013 framework dictates that all above features must be primary in the document and as such have been carefully analyzed and made part of the ISMS>

# Monitoring (Clause 8 & 9)

After planning and implementing the ISMS, it is necessary to make sure that the employees of Garkeens Supermarket follow the procedures, protocols and doctrines documented within the Information Security Management System. This section of the document will go into in-depth explaination as to how and what to do in order to ensure that the ISMS is in full effect. The security staff is entirely responsible for updating and ensuring the procedures documented below are put into effect.

## Tools and procedures that will assist in monitoring

### Auditing (External or Internal)

The simplest and the least complex but the most essential monitoring procedure that must be put into effect is audits. Security audits are the process by which an entire foolproof checkup is performed on the entire system that the ISMS has been put into place to ensure the security of.

Some advantages and disadvantages of audits are:

* External audits may result in data breaches as the party does not gain anything by ensuring the security of Garkeens Supermarket.
* Internal audits are biased towards the Garkeens Supermarket and will often yield insufficient or insiginificant conclusions that will assist in understanding the security standpoint of the organization.
* Audits give the complete overview of where an organization stands when it comes to security.
* Audits often reveal security threats and risks, these can be identified and then necessary actions can be taken in order to ensure that it does not damage Garkeens Supermarket.

All audits both external and internal must perform the following procedures by minimum:

* Port scanning
* Going through logs and documenting findings
* Interviewing the senior and assistant security head to know if the lower levels of the hierarchy are functioning optimally.
* Intervieiwing the department heads individually to know if the upper levels of the hierarchy are functioning optimally.
* Risk Scoring/Assesment if risks or threats have been found
* Check that all software and hardware are of the Latest Stable version and have no security vulnerabilities themselves.
* Check that anti-virus programs are running in their configured timetables and also if the time tables are accurate.
* Check that all hardware have been properly maintained.
* Check if management is being properly notified of the ongoing of the security within Garkeens Supermarket.

## Various software that can be used to monitor the system

These software are industrially accepted and have lincensing specially for industrial usages. Upon contacting the companies that sell these software, they will provide Garkeens Supermarket with a solution perfectly unique to the nature of Garkeens Supermarket:

1. Solarwinds Network Performance Tool – This software visualizes all devices that are connected to the Garkeens Supermarket network system and essentially can be used to ensure that no device other than company authorized and tested devices will be injected to the network. The tool is very customizable and will serve greatly in the network administration of the Information Security Management System.
2. ManageEngine OpManager- This software is capable of understanding the suspicious activity of an application, if a virus has infected a device, this tool will immediately disconnect the device from the network until the network administrator accepts the device back in.
3. MalwareBytes – The best anti-malware, virus and rootkit software in the industrial space. With regular updates to their databases, MalwareBytes is capable of ensuring high security standards. It comes with both web and network security, real-time protection, boot-protection, device protection and mail protection.
4. Wireshark – This is a packet analyzer, that will grant the security senior head of Garkeens Supermarket of the ongoings within the network. Analyzing the packet flow within a network will making sure things like attacks to the mailing server and MIS don’t happen.
5. Metasploit – This is a large security project that helps to identify security vulnerabilities and aids in penentration testing in order to help patching up vulnerabilities within the system. It is capable of so many various things that it is ranked among one of the best penetration testing tools in the world.
6. Aircrack-NG – This is a networking software suite that consists of detecting, packet sniffing, WEP and WPA/WPA2-PSK cracking and analysis features. It can be used on various wireless networks like 802.11b, 802.11g etc.

# Improvements (Clause 9)

Possible improvements to the existing Information Security Management System are:

* Additional nodes within the hierarchy that will take away the workload the senior and assistant security head have to perform.
* Toning down or catering the Information Security Management System based on statistics and opinions of the employees of Garkeens Supermarket.
* Centralizing information within the Garkeens Supermarket Information System and basing all security devices and software to protect that centralized node, which will significantly decrease the budget and the time that is needed in order to ensure that the ISMS is functioning efficiently.
* Reducing quantity of security products and using products that provide more than one feature which will reduce the risk of the vulnerabilities of each security product.
* Maintaining a specific department for security, than just using the IT staff. This will require more employees but is guaranteed to grant security of the highest level as they can focus entirely on the security of Garkeens Supermarket.
* Investing more on awareness, training and orientation programs in order to fully equip every employee within Garkeens Supermarket with the required information to process the security situation within the Garkeens Supermarket.

## How does ISO align with the controls and procedures used for monitoring and improvement?

These monitoring procedures and controls are in compliance with the ISO:31000:2013 security framework that is responsible for risk assessment, security policies and monitoring a security system.

The following principles of ISO:31000:2013 monitoring clauses and ISO:27001:2013 monitoring clauses have been deeply entrenched within the document:

* All monitoring tools must be industrially accepted.
* All monitoring tools and procedures must be of the most stable and secure versions.
* Auditing must be the primary monitoring procedure and tool that will help and allow the security system to function to it’s optimum that is per the ISMS.
* Whenever a monitoring tool is introduced, it must be discussed briefly and the features it provides and the scope must be provided.
* All monitoring tools that expose sensitive data must be used by the higher levels of the hierarchy responsible for the security of a company.
* The usage of monitoring tools must be and only for monitoring. The tools must not be used for any illegal actions for personal desires or educational purposes.
* Any tool with the potential of harming the system must be used with utmost care. Backups must be readily in place before using a monitoring tool that has the potential of harming the system.

# Advantages and disadvantages of ISO:27001:2013

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| * Protects information from going to unauthorized personnale. * Ensures information is accurate, upto date and is accessible and can be modified by only the authorized users of Garkeens Supermarket. * Asses the impacts and vulnerabilities of a particular risk. * The ISO:27001:2013 has been announced as one of the best security standards, this gives a sense of trust and comfort to all customers of Garkeens Supermarket. * Increases the reliability and quality of company resources. * Gives comfort and trust to all business partners of Garkeens Supermarket, which will lead to a phase where the business thrives and there’s stakeholders for the company to economically function optimally. * Gives a more “hands-on” approach for all employees of Garkeens Supermarket when it comes to handling issues within the system. * Ensures that Garkeens Supermarket is not just a business, but also a community that listens to the needs and requirements of its fellow customers and clients. * Improves the management of company resources and reduces the money spent on recovery procedures and damage control. * Helps organizing the company in a better and smarter manner based on the practices that have been proven to work for countless other organizations like Garkeens Supermarket. | * Implementing an ISMS is both budget wise and time wise, extremely difficult. * The designed Information Security Management System document can only be used by Garkeens Supermarket as it has specifically been produced to solve the problems within this organization. * It is always difficult how to scope and how far to scope the regulations and protocols set for an organization. * It is possible to mislead the customers that are technologically challenged that the organization is being too strict for unnecessary reasons which can result in bad image. * It is always difficult for any employee that is not technologically knowledge to live upto the standards and expectations of a document, no matter how many trainings or awareness programs the organization does, there is always a possibility that an employee will perform a mistake that may result in large problems, which almost makes the ISMS look pointless to implement. * The International Standard Organization’s officers are quite strict in terms of ensuring the standards of the ISO:27001:2013 being implemented in an organization. In case ISO decides to decertify an organization, this could result in a large blow the image and reputation of an organization. |

# ISO:27001 vs other security standards

ISO:27001 is a general security framework that is concerned with protecting the information system of an organization however though there are other security standards that are more within scope of Garkeens Supermarket which are:

* ISO:22004 – A security framework concerned with managing food safety, as Garkeens is a supermarket, the highest consumable product within the supermarket is foods. As such ISO:22004 is more applicable to the context however though ISO:27001 ensures that management behind the management of food is processed properly.
* ISO:10377 – A security framework concerned with managing the safety of products, this involves that the products of Garkeens supermarket meet quality standards, are delivered on time and that the suppliers of Garkeens Supermarket meets the industrial consumer product standard according to ISO. ISO:27001 however is responsible with ensuring that these suppliers interact with the system of Garkeens Supermarket in a secure and a responsible manner.
* ISO/IEC DIS 19770-1 : An information technology based security framework that is more concerned with asset prioritization, importance, identification and securing. It is concerned with managing the assets of a business organization, which is something ISO:27001 also attempts to do, but focusing less on prioritization, importance or identification but on security of assets.

|  |  |
| --- | --- |
| **Bibliography** | |
| International Standards Organization | <https://www.iso.org/management-system-standards-list.html> |
| Search security: Tech Target | [https://searchsecurity.techtarget.com](https://searchsecurity.techtarget.com/) |
| Reddit (r/security) | <https://www.reddit.com/r/security/> |
| Reddit (r/sysadmin) | <https://www.reddit.com/r/sysadmin/> |