JANUARY 2018

ISO 27000 COMPLIANCE

USING SEPIO VISIBILITY AND POLICY ENFORCEMENT SOFTWARE SUITE

SOLUTION BRIEF

PREPARED BY:

Bentsi Ben Atar

www.sepio.systems
US: 11810 Grand Park Ave., Rockville, MD 20852
Israel: 63 Rothschild Blvd., Tel-Aviv, 6578510

WHAT THIS IS ALL ABOUT

ISO 27000

ISO bundles its standards into subject-specific series, such as ISO 27000, which describes best practices for an Information Security Management System - ISMS.

ISO 27001

The ISO/IEC 27001 standard (shared between the ISO and IEC) is designed to help organizations keep their data safeguarded against intrusion and/or theft.

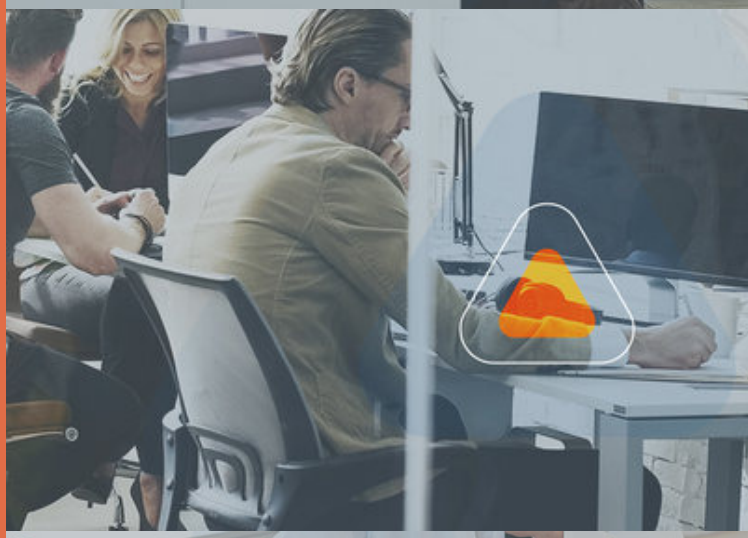
ISO 27002

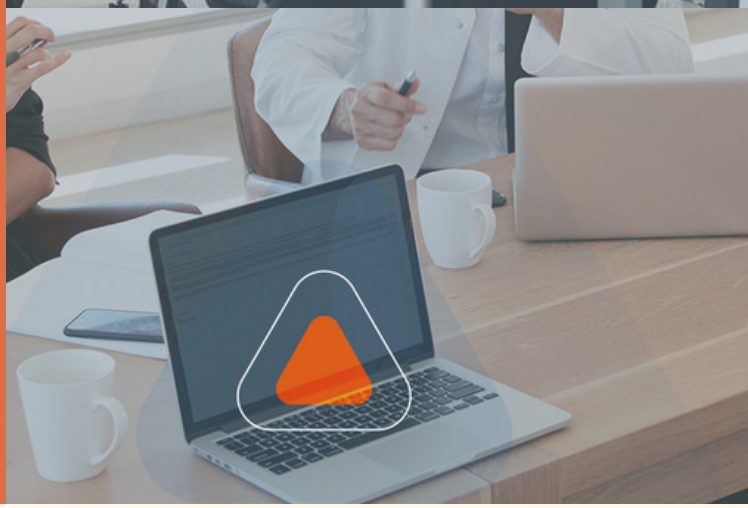
The ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining information security management systems.

Methodology

The standard uses a topdown, risk-based approach, and lists six steps to create and test your systems for an optimized ISMS:

- Create your policy to protect data.
- Establish the parameters of your ISMS.
- Carry out a risk assessment.
- Determine how to resolve vulnerabilities.
- Decide what controls are intended to achieve and which ones to enact.
- Write out any deployment decisions and refinements to set the ISMS into action.





REASONING & BENEFITS

A quick look at the effects of being ISO 27001 compliant.

ISO 27001 is an international management standard that provides a proven framework for managing information security, using an integrated set of recommended policies, procedures, documents and technology in the form of an ISMS (information security management system).

Through its all-encompassing approach, an ISMS aligned to ISO 27001 can help an organisation protect all of its corporate information and intellectual property, not just its personal data.

ISO 27001 compliance means a business has taken steps to regularly identify and manage its data security risks. In so doing, it is able to keep up with constantly evolving data security threats.
ISO 27001 provides guidance for implementing appropriate measures to mitigate those risks.

Achieving ISO 27001 certification can also provide convincing evidence that you have taken the necessary measures to comply with the data security requirements of the GDPR.

Compliance benefits:

- Determine any vulnerabilities and implement plans to resolve or minimize.
- Choose mechanisms that work best.
- Communicate with partners and clients and ease their security concerns.
- Comply with regulations and earn greater vendor credibility.
- Decrease your liability.

The following sections detail regulation requirements and recommendations from the standard and will point out how the Sepio Solution helps addressing them

ISO/IEC 27002:2013 STRUCTURE

The standard lists 114 Information Security controls divided over 14 chapters, but not all controls are equally relevant for all organizations

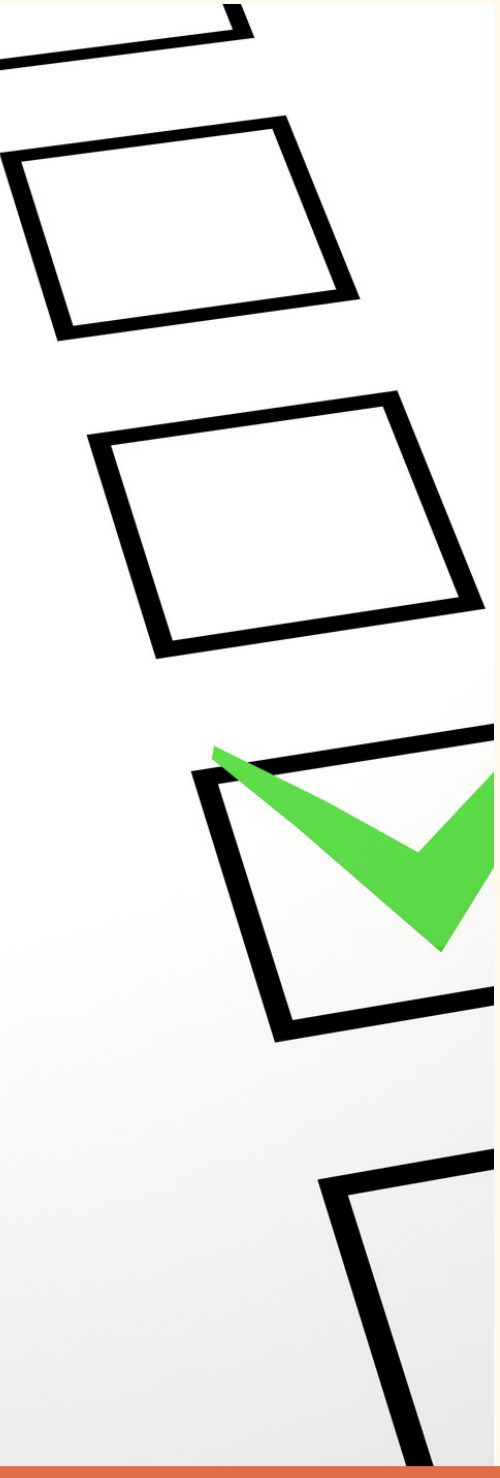
SCOPE AND THE RELEVANT SECTIONS

ISO 27001 defines the mandatory requirements for an Information Security Management System.
ISO 27002 indicates suitable information security (IS) controls within the ISMS.

- (6) Organization of Information Security.
- (8) Asset Management.
- (11) Physical and environmental security.
- (12) Operation Security- procedures and responsibilities, Protection from malware, ... Logging and monitoring, Control of OS, ... Technical vulnerability management and IS audit coordination.
- (13) Communication security - Network security management and Information transfer.
- (15) Supplier relationships - Information security in supplier relationships.
- (16) IS incident management - Management of incidents and improvements.
- (18) Compliance - Compliance with legal and contractual requirements and IS reviews.

ISO/IEC 27002 HAS DIRECTLY EQUIVALENT NATIONAL STANDARDS IN 26 COUNTRIES

ANALYSIS



SECTION 6:

ORGANIZATION OF INFORMATION SECURITY

6.2 Mobile devices and teleworking

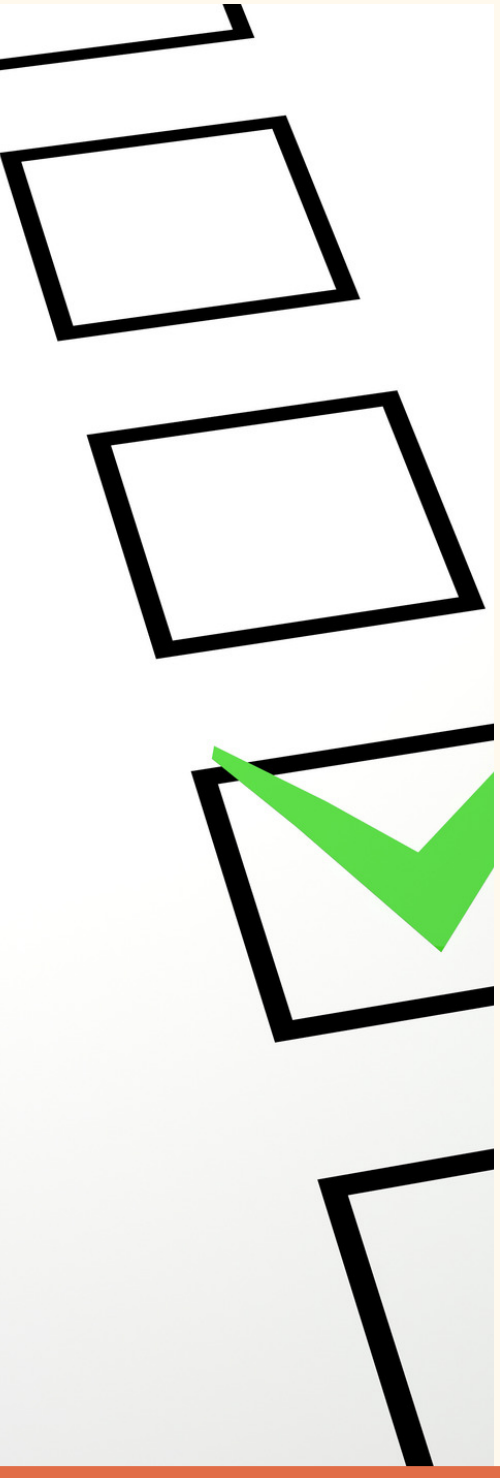
There should be security policies and controls for mobile devices (such as laptops, tablet PCs, wearable ICT devices, smartphones, USB gadgets and other Boys' Toys) and teleworking (such as telecommuting, working-from home, road-warriors, and remote/virtual workplaces).

The Sepio security suite allows the user to define and enforce a hardware usage policy per specific device type or even the interface level (part of the functionality)

ANALYSIS

SECTION 8:

ASSET MANAGEMENT



8.1 Responsibility for assets

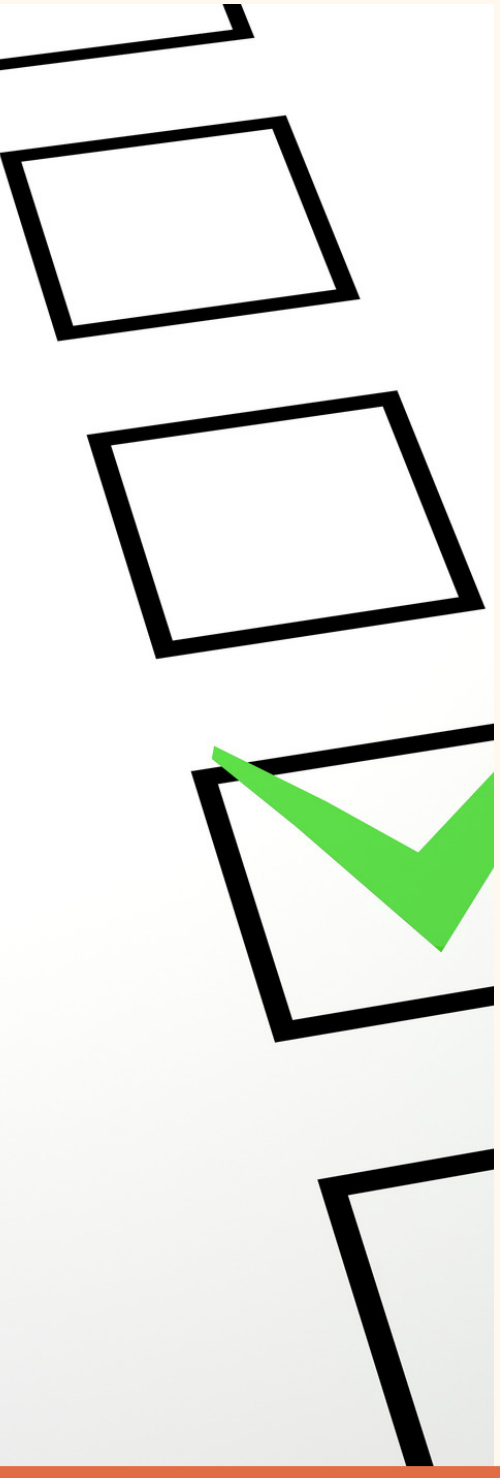
All information assets should be inventoried and owners should be identified to be held accountable for their security. 'Acceptable use' policies should be defined, and assets should be returned when people leave the organization.

The Sepio security suite provides the user with full visibility to connected device. When policy enforcement is enabled, it will automatically disable any asset that breaches the defined policy or belongs to people that are leaving the organization.

ANALYSIS

SECTION 8:

ASSET MANAGEMENT



8.2 Information classification

Information should be classified and labelled by its owners according to the security protection needed, and handled appropriately.

8.3 Media handling

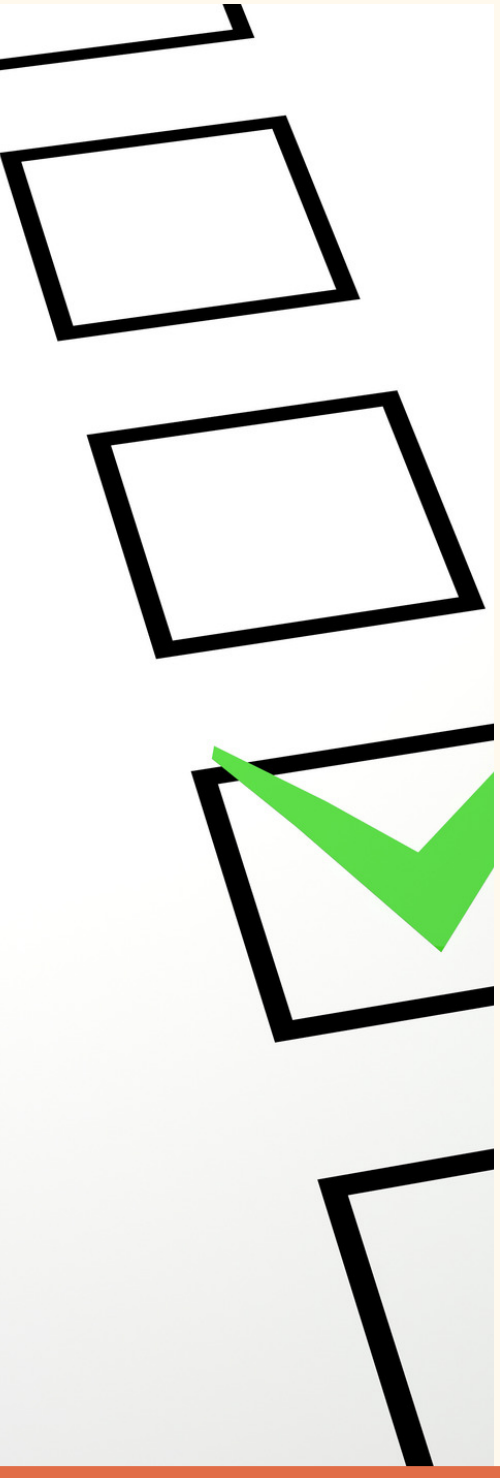
Information storage media should be managed, controlled, moved and disposed of in such a way that the information content is not compromised.

The Sepio security suite provides the user with the means for managing storage assets containing protected information.

ANALYSIS

SECTION 11:

PHYSICAL AND ENVIRONMENTAL SECURITY



11.2 Equipment

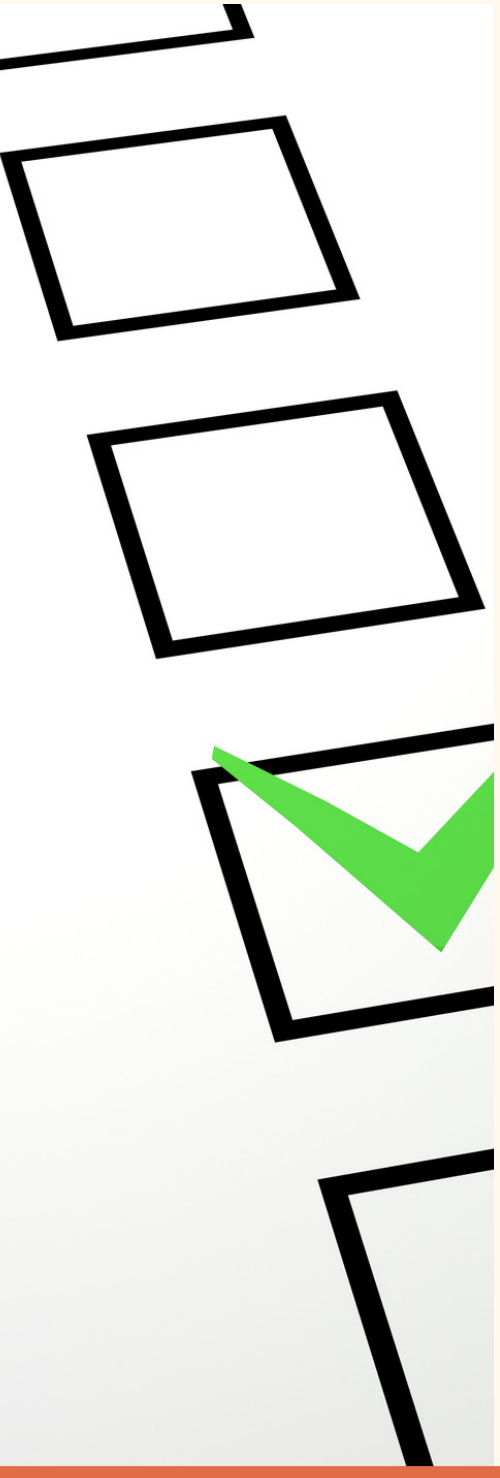
"Equipment" (meaning ICT equipment, mostly) plus supporting utilities (such as power and AC) and cabling should be secured and maintained.
Equipment and information should not be taken off-site unless authorized, and must be adequately protected both on and off-site. Information must be destroyed prior to storage media being disposed of or re-used. Unattended equipment must be secured and there should be a clear desk and clear screen policy.

The Sepio security suite provides full visibility to the organization's assets and supports all required policies.

ANALYSIS

SECTION 12:

OPERATIONS SECURITY



12.4 Logging and monitoring

System user and administrator/operator activities, exceptions, faults and information security events should be logged and protected. Clocks should be synchronized.

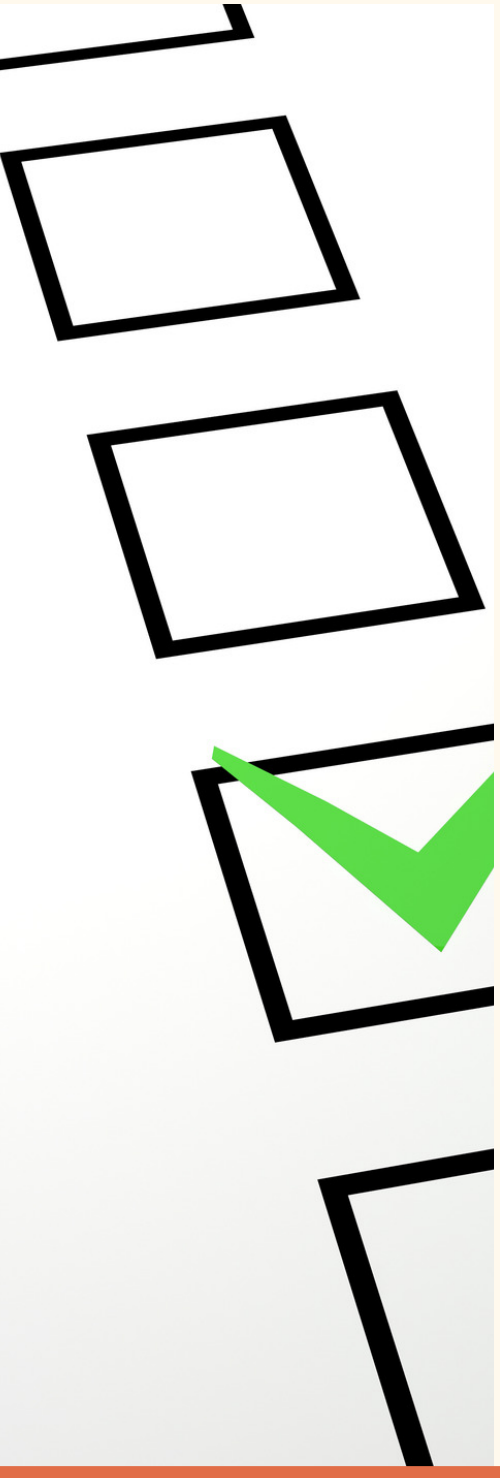
The Sepio security suite keeps a full audit trail for any user activity and information regarding security events.

12.6 Technical vulnerability management

Technical vulnerabilities should be patched, and there should be rules in place governing software installation by users.

Based on its threat intelligence collection capabilities, The system provides the user with up-to-date vulnerability information related to the organization's assets.

ANALYSIS



SECTION 12:

OPERATIONS SECURITY

12.7 Information systems audit considerations

IT audits should be planned and controlled to minimize adverse effects on production systems, or inappropriate data access.

The Sepio security suite keeps a full audit trail for any user activity and all IS events.

SECTION 13:

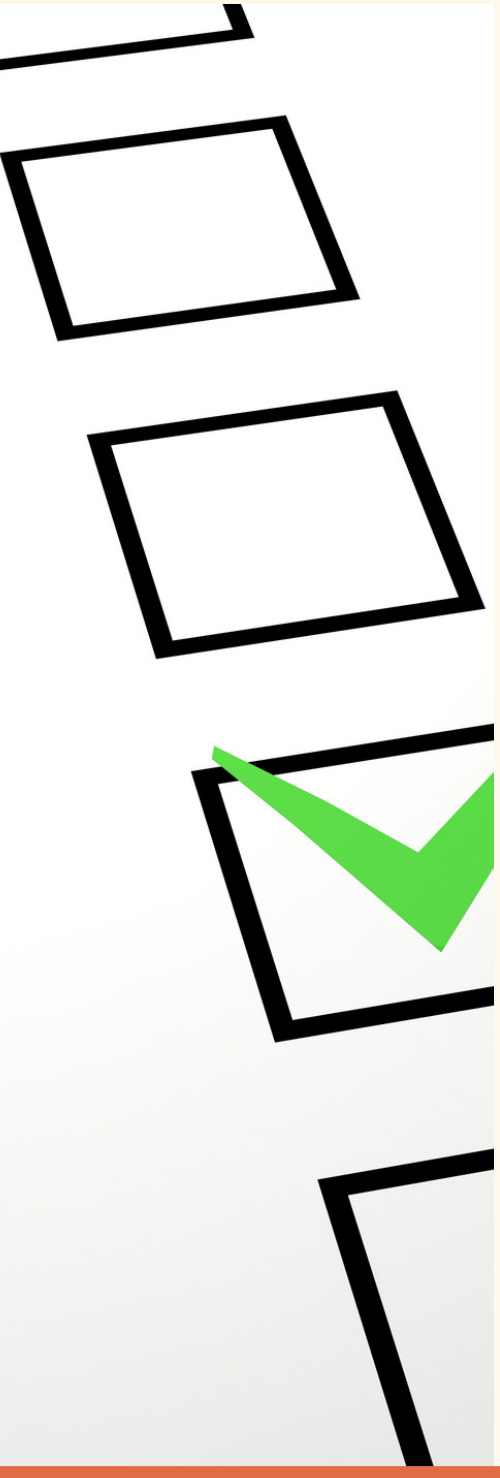
COMMUNICATIONS SECURITY

13.1 Network security management

Networks and network services should be secured, for example by segregation.

The system keeps the network strictly sanitized from devices that can infect or invisibly leak data from the network.

ANALYSIS



SECTION 15:

SUPPLIER RELATIONSHIPS

15.1 IS in supplier relationships

There should be policies, procedures, awareness etc. to protect the organization's information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed within the contracts or agreements.

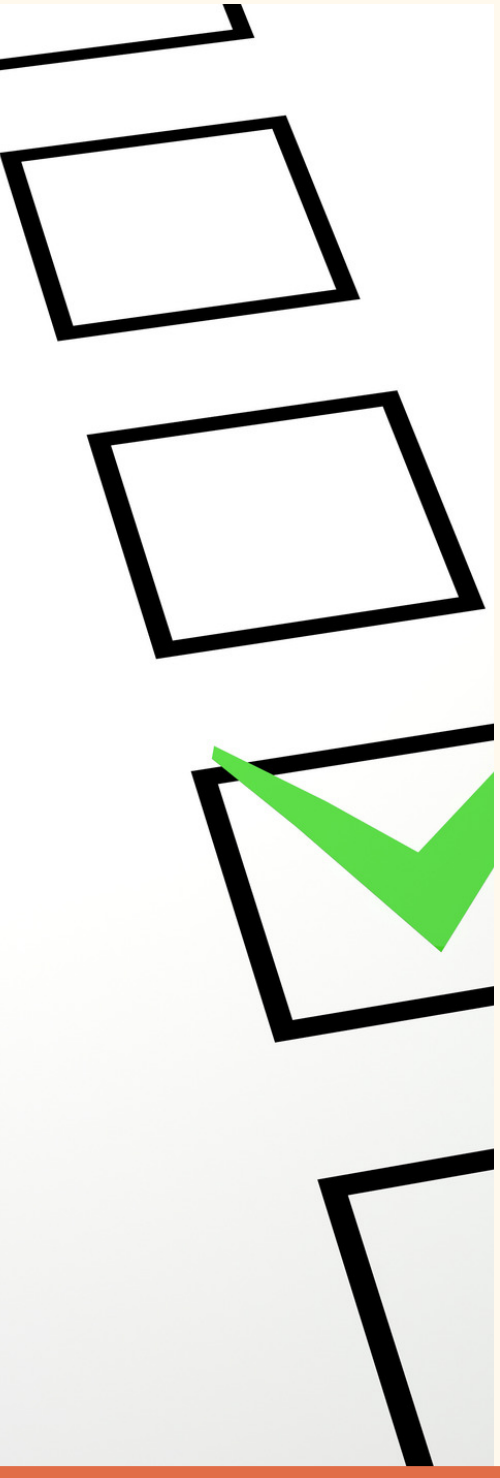
The Sepio suite supports multiple policies that monitors and can limit access to the organization's assets.

15.2 Supplier service delivery management

Service delivery by external suppliers should be monitored, and reviewed/audited against the contracts/agreements. Service changes should be controlled.

The system tracks all changes in the organization's assets in real time and keep audit trails for any issued activity.

ANALYSIS



SECTION 16:

INFORMATION SECURITY INCIDENT MANAGEMENT

16.1 Management of information security incidents and improvements

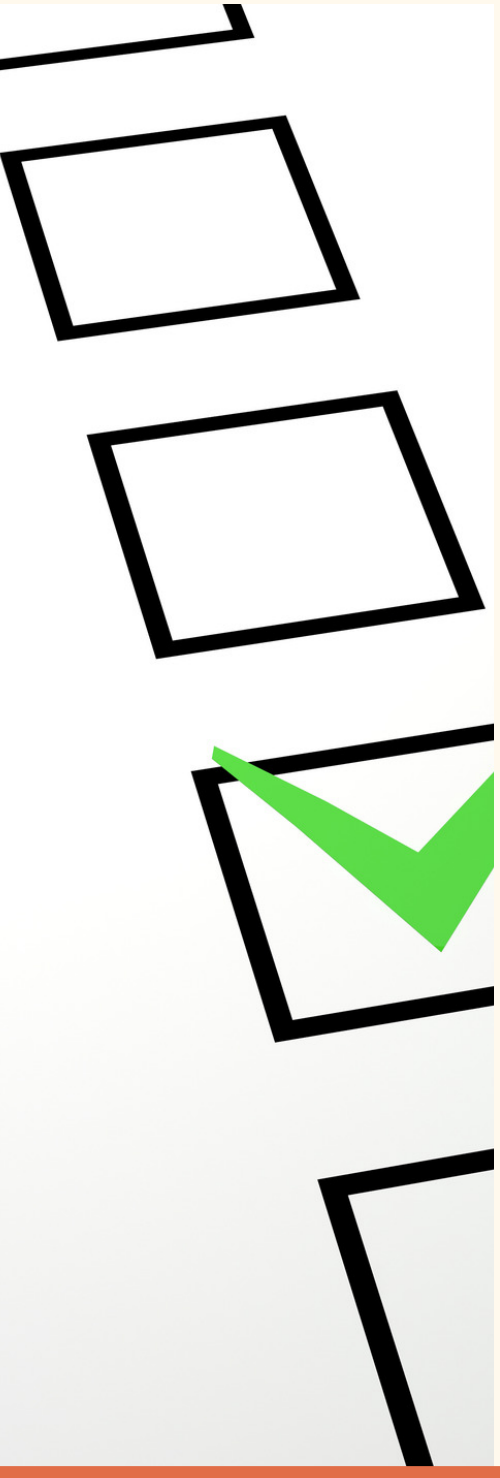
There should be responsibilities and procedures to manage (report, assess, respond to and learn from) information security events, incidents and weaknesses consistently and effectively, and to collect forensic evidence.

The Sepio suite monitors and manages all security events information supporting reporting tools and creation of common organizational knowledge base.

ANALYSIS

SECTION 18:

COMPLIANCE



18.2 Information security reviews

The organization's information security arrangements should be independently reviewed (audited) and reported to management. Managers should also routinely review employees' and systems' compliance with security policies, procedures etc. and initiate corrective actions where necessary.

Sepio Prime continuously enforces the user set policy and alerts upon compliance breaches the moment they occur.

RECAP

Why should your organization adopt ISO 27000 and how you can benefit from deploying the Sepio solution

The business benefits from ISO 27001 certification are considerable. Not only do the standards help ensure that a business' security risks are managed cost-effectively, but the adherence to the recognized standards sends a valuable and important message to customers and business partners:
This business does things the correct way.

ISO 27001 is the de facto international standard for Information Security Management and demonstrates a clear commitment to Information Security Management to third parties and stakeholders. It can provide a framework to ensure the fulfillment of commercial, contractual and legal responsibilities, and provides a significant competitive advantage.

Organizations are relatively protected against cyber-attacks on their networks, applications and data infrastructure. However, very few are focused on hardware devices as attack vehicles for penetrating their infrastructure, infecting their computers, and stealing sensitive information.
The Sepio security suite provides full visibility into all hardware assets in the network, and allows administrators to define and easily enforce their security policy. Having the Sepio solution installed helps keeping the network hygiene. Immediate alerting, comprehensive visibility, reports, and security dashboards act as an effective tool set for keeping compliance with many of the information security controls that are recommended in the standard.

DATE Jan 17, 2018
VER 1.01.12