Smart Information Security Management System Tool (SISMS-Telecommunications)

Fulfilling the requirements of ISO/IEC 27011 Information technology -- Security techniques -- Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations Standard of which's usage is growing up worldwide day by day, requires information and experience on it. On the other hand getting consultancy services usually comes with high costs. The reason for the complexity of processes you need consultancy or expert personnel to work with.

Cymsoft's Smart Information Security Management System for Telecommunications Organizations so called SISMS-Telecommunications is a tangible indicator of Cymsoft's experience on establishing SISMS-Telecommunications is a R&D project supported by The Scientific and Technological Research Council of Turkey (TUBITAK). SISMS-Telecommunications is a software which is developed to make it easier in accomplishing the whole processes of ISO/IEC 27011 using artificial intelligence.

SISMS-Telecommunications fulfills all requirements in ISO/IEC 27011 and provides compliance with the Standard.

Through Information Security Management process, the software package encapsulates following modules;

- Scope,
- Information Security Policy,
- Inventory of Assets,
- Risk Evaluation Methodology,
- Risk Analysis,
- Risk Management,
- Gap Analysis,
- Mandatory Procedures,
- Document Management,
- Protective Controls,
- Compliance Monitor,
- Corrective and Preventive Activities Maintenance.

GAP Analysis

- A test application which defines how to apply controls to determine organization's compliance with ISO/IEC 27011 Standard and make complex rules of ISO/IEC 27002 Standard to be understood easily,
- Management of Controls in ISO/IEC 27011 forming the infrastructure of test application and management of rules in ISO/IEC 27002 corresponding the application of controls,
- Updatable rule base according to ISO/IEC 27011 and ISO/IEC 27002 Standards' requirements,
- Documentation of conformities and unconformities resulting test application,
- Preparing a substructure towards automated documentation of mandatory procedures of ISO/IEC 27011 Standard, resulting test application,
- Providing a Maturity Model that shows compliance of the organization visually.

SISMS-Telecommunications;

Make it easy to understand and use the abstruse and complex structure of ISO/IEC 27000 Standards family with application of artificial intelligence.
Has a feature of cost reducing and Standard/Quality enhancement on establishing ISMS.

Distinguishing Characteristics of ISMS-Telecommunications;

- Detecting hardware assets on network and recording assets manually,
- Collecting and evaluating the assets under an asset group (top asset),
- Calculating the asset values with three different method,
- Usage of five different risk evaluation methodologies four of which qualitative (including Octave Allegro) and one quantitative.
- Automated determination of threats, vulnerabilities and risk values of assets (including asset groups) according to asset categories,
- Ability of adding own asset categories,
- Information asset types identified, categorized and updatable thread and vulnerability types related with these assets types on system,
- Automated determination of protective controls against the vulnerabilities towards information assets,
- Ability of adding own protective controls and relating them with threats,
- Preparation of Inventory of Assets, Risk Evaluation Report and Statement of Applicability (SoA),
- Ability to perform Gap Analysis,
- Automated documentation of mandatory documents included in the Standard,
- Multilanguage and help support,
- Defining different user roles,
- Defining different authentication for different types of roles,
- LDAP integration for user management,
- Defining organizational title, business sector, company logo, address information, hierarchical organization unit chart, and business processes,
- Defining correlation between assets, business processes and organizational units,
- User friendly web based software,
- Low cost advantage.

Cymsoft Information Technologies.
Remzi Oğuz Arık Mah. Şimşek Sok. No.19/4 06680 Kavaklıdere / ANKARA /TURKEY
Tel : +90 312 2650525 Faks : +90 312 2650331 info@cymsoft.com www.cymsoft.com

SISMS-TELECOMMUNICATIONS MODULES

CYMSOFT BİLİŞİM TEKNOLOJİLERİ

Inventory of Assets

- Tracing software and hardware assets on Local Area Network and inserting them into inventory database automatically,
- Importing existing asset inventory in excel form appropriate to software in case it's not desirable to search the information assets on Local Area Network,
- Inserting information assets which are not connected on Local Area Network into inventory database manually using asset entry interface,
- Assigning assets to more than one business processes or correlating business processes with more than one asset,
- Defining asset groups for collecting the assets having same qualification under a unique asset group and managing them all together,
- An interface of which asset category, asset group, asset location, asset owner and asset explanation can be monitored and asset can be correlated to business processes,
- Defining confidentiality, integrity and accessibility values of assets one by one or under an asset group as maximum, sum or multiplication (optional) values.
- Keeping track of asset owners on unit base and listing assets on category or process base.
- Detailed documentation of asset inventory.

Risk Management

- Automated assignment of vulnerabilities and related threats of assets, according to their classification, without user intervention by the system,
- Defining Protective Controls against to vulnerabilities and threats,
- Five optional qualitative and quantitative risk evaluation methodologies you can choose dynamically:
  - ISO/IEC 27005 Risk Evaluation Methodology-1,
  - ISO/IEC 27005 Risk Evaluation Methodology-2,
  - Probabilistic Risk Evaluation Methodology,
  - Octave Allegro Evaluation Methodology,
  - Quantitative Risk Evaluation Methodology.,
  - Risk analysis application with different risk evaluation methods taking into account the values; Asset Value-AV, Exposure Factor-EF, Single Loss Expectancy-SLE, Annualized Rate of Occurrence-ARO, Annualized Loss Expectancy- ALE ,
- Ease of performing risk analysis with optional risk evaluation methodologies,
- Documentation of Risk Evaluation Report in excel format appropriate to ISO/IEC 27011 Standard,
- Graphical presentation of risk positions of organization's information assets according to their classification "Risk Analysis Table"

Protective Controls

- Improving organization's ISMS in course of time;
  - List of conformities and unconformities after Gap Analysis,
  - Defining controls from ISO/IEC 27011 and 27002 for nonconformities.

Document Management

- Document importing, exporting and monitoring according to user authority,
- Versioning and keeping documents by date and publishing the current version on web page,
- Producing the mandatory documents listed below for ISO/IEC 27011 certification automatically and allowing to update them only by authorized (Administrator) user,
- Publishing the prepared documents, presenting all documents to users which will be able to access on the organization's local portal,
- Presenting all required templates,
- Documents that can be produced by the software;
  - Information Security Policy,
  - ISMS Scope,
  - Controls and procedures supporting ISMS;
    - √ Risk Evaluation Procedure,
    - √ Organization of Information Security Procedure,
    - √ Human Resource Security Procedure,
    - √ Asset Management Procedure,
    - √ Access Control Procedure,
    - √ Physical and Environmental Security Procedure,
    - √ Communications and Operations Security Procedure,
    - √ System Acquisition, Development and Maintenance Procedure,
    - √ Information Security Incident Management Procedure,
    - √ Information Security Aspects of Business Continuity Management Procedure,
    - √ Compliance Procedure,
    - √ Business Continuity Plan,
  - Asset Inventory,
  - Risk Analysis Report,
  - Risk Evaluation Report,
  - Statement of Applicability (SoA),
  - Other required records which are evidence of compliance and effective performance of ISMS;
    - √ Internal Audit Procedure,
    - √ Control of Documents and Records Procedure,
    - √ Corrective and Preventive Activities Procedure,
    - √ Document List,
    - √ Internal Audit Questions Lists,
    - √ Management's Review Report.

Compliance Check

- A dashboard checking requirements in documentation with their last versions and presenting compliance level of the organization.
- Providing top management to review whole ISMS.

Internal Audit

Related with internal audits;

- Selecting units to be audited,
- Selecting auditors,
- Question lists, planning and tracing audit activities.

Corrective and Preventive Activities

- Managing Corrective and Preventive Activities on system,
- Assigning personnel for each activity, monitoring activities, following deadline for each activity, and closing the activity if compliance is provided,
- Listing all open activities for management's review report.

KOSGEB

Cymsoft Information Technologies.
Remzi Oğuz Arık Mah. Şimşek Sok. No.19/4 06680 Kavaklıdere / ANKARA /TURKEY
Tel : +90 312 2650525 Faks : +90 312 2650331 info@cymsoft.com www.cymsoft.com