Journal of
Improvement Management
Vol. 10 No. 4, Winter 2017 (Serial 34)

The Impact of IT Security in the Implementation of Knowledge Management System

Davood Sheikhali[1], Reza Hosnavi[2]☎, Majid Ramezan[3]

1- MSc in Information Technology Management, Faculty of Management, Islamic Azad University E-Campus, Tehran, Iran.
2- Associate Professor, Faculty of Management and Industrial Engineering, Malek Ashtar University of Technology, Tehran, Iran.
3- Assistant Professor, Faculty of Management and Industrial Engineering, Malek Ashtar University of Technology, Tehran, Iran.

Abstract:

One of the organization concerns is security in implementing knowledge management system. The purpose of this study is investigating the effect of IT security according to ISO/IEC27001:2013 in the implementation of secure knowledge management system. This research from the method perspective is descriptive-survey and from the goal perspective is practical. The required information through library studies, interviews and paired comparisons questionnaires have been collected. The hybrid method DEMATEL and ANP is used to determine the causal and prioritize control objectives of this standard in regards to knowledge management system.

Research findings indicate a causal relationship between control objectives of ISO/IEC27001:2013 in the knowledge management system establishment. Also information security organization, operations security, communications security and encryption have higher priority than the other control objectives of this standard.

***Keywords**: Information Security, Knowledge Management.*

1. iauecms@gmail.com
2. ☎*Corresponding author:* hosnavi@mut.ac.ir
3. m_ramezan83@yahoo.com

نشریه علمی – پژوهشی بهبود مدیریت
سال دهم، شماره ۴، پیاپی ۳۴، زمستان ۱۳۹۵
صفحات ۴۷ - ۲۵

بررسی تأثیر امنیت فن‌آوری اطلاعات در اجرای سامانه مدیریت دانش

(تاریخ دریافت: ۹۵/۰۴/۰۷ تاریخ پذیرش: ۱۳۹۵/۱۰/۲۸)

داود شیخعلی[۱]، رضا حسنوی[۲*]، مجید رمضان[۳]

چکیده

یکی از دغدغه‌های سازمان‌ها، اجرای امن سامانه مدیریت دانش است. بر این اساس، هدف پژوهش حاضر، بررسی تاثیر امنیت فن‌آوری اطلاعات طبق استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ در اجرای امن سامانه مذکور است. این تحقیق از نظر روش، توصیفی- پیمایشی و از نظر هدف، کاربردی است. اطلاعات مورد نیاز از طریق مطالعات کتاب‌خانه‌ای، مصاحبه و پرسش‌نامه مقایسات زوجی جمع‌آوری شده است. روش ترکیبی دیمتل و فرایند تحلیل شبکه‌ای برای تعیین اثرگذاری یا اثرپذیری و اولویت‌بندی اهداف کنترلی استاندارد فوق در ارتباط با سامانه مدیریت دانش استفاده گردیده است. یافته‌های پژوهش، بیانگر ارتباط علی و معلولی بین اهداف کنترلی ISO/IEC۲۷۰۰۱:۲۰۱۳ در استقرار سامانه مدیریت دانش است. همچنین، اهداف کنترلی تشکیلات امنیت اطلاعات، امنیت عملیات، امنیت ارتباطات و رمزنگاری از استاندارد مذکور دارای اولویت بالاتری نسبت به سایر اهداف کنترلی استاندارد فوق هستند.

واژگان کلیدی:
امنیت اطلاعات، مدیریت دانش

۱- کارشناس ارشد مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی واحد الکترونیکی، دانشکده مدیریت، تهران iauecms@gmail.com
۲*- دانشیار دانشگاه صنعتی مالک اشتر (نویسنده مسئول): hosnavi@mut.ac.ir
۳- استادیار مجتمع دانشگاهی مدیریت و فناوری‌های نرم دانشگاه صنعتی مالک اشتر، تهران ramezan@mut.ac.ir

۱- مقدمه

بسیاری از سازمان‌ها، فن‌آوری اطلاعات را به یک شکل خاص یا اشکال مختلف برای مدیریت دانش خود مورد استفاده قرار می‌دهند. مدیریت دانش می‌تواند با استفاده مناسب از فن‌آوری اطلاعات، نتایج بسیار مهمی را به‌دنبال داشته باشد[۲]. مبادلهٔ اطلاعات، دسترسی آسان به داده‌ها و ارتباط از راه دور، کارکنان یک سازمان را قادر می‌سازد تا واحد کاری خود را به‌طور پویا در موقعیت‌های جغرافیایی و ابعاد زمانی متفاوت ایجاد کنند. بنابراین، یک سازمان می‌تواند شانس بهتری در تبدیل شدن به کلاس جهانی به واسطهٔ انعطاف‌پذیر بودن و مجازی بودن داشته باشد[۴]. سازمان‌ها برای بقا و پیشرفت به سیستم‌های اطلاعاتی نیاز دارند، در نتیجه باید به‌طور جدی به حفاظت از دارایی‌های اطلاعاتی خود بپردازند. ایجاد تبادلات ساختارمند و توجیه‌پذیر بین هزینه، امنیت و مأموریت برای کنترل مخاطرات سیستم‌های امنیتی، ضروری است. این امر در برنامه‌ریزی و توسعهٔ چنین سیستم‌هایی از اهمیت ویژه‌ای برخوردار است[۱].

در سال‌های اخیر، بحث بهره‌برداری از قابلیت‌های فن‌آوری اطلاعات و ارتباطات به‌عنوان عاملی توانمندساز و تسهیل‌گر در فرآیندها، مورد توجه سازمان‌های ایرانی قرار گرفته است. یکی از مهم‌ترین عوامل تاثیرگذار در به‌کارگیری قابلیت‌ها و توانمندی‌های فناوری اطلاعات و ارتباطات به‌ویژه در صنایع نظامی، مقوله حفظ امنیت اطلاعاتی است که در این بستر قرار داده می‌شود.

معمولاً سازمان‌های صنعتی و فن‌آوری‌محور برای افزایش نرخ نوآوری محصولات خود تلاش می‌کنند. مدیریت دانش یکی از راه‌کارهای افزایش نرخ نوآوری است و یکی از تصمیمات سازمانی در این راستا تهیه و عملیاتی نمودن سامانه‌ای برای مدیریت دانش است. در این قبیل سازمان‌ها دانش‌های زیادی تولید می‌گردد، اما اشتراک آن مشکلات زیادی دارد. یکی از مهم‌ترین چالش‌های آن مربوط به امنیت اطلاعات به‌ویژه در سامانه‌های نرم‌افزاری است. این موضوع به‌ویژه در سازمان‌های نظامی سبب کندی فرایند استقرار آن می‌گردد. با اجرای استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳، یکی از مسایل مطرح شده برای مدیران این است که استقرار آن تا چه میزان می‌تواند دغدغه‌های ناشی از امنیت سامانه مدیریت دانش را برطرف نماید. همچنین رتبه‌بندی میزان تاثیر هر یک از اهداف کنترلی استاندارد مذکور بر سامانه مدیریت دانش به چه صورت خواهد بود تا براساس آن مدیران بتوانند برای تهیه و عملیاتی نمودن آن، تصمیم‌گیری بهتری داشته باشند.

هدف اصلی این پژوهش، بررسی تاثیر امنیت فناوری اطلاعات براساس استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ در اجرای سامانه مدیریت دانش است، با توجه به آن، حصول اهداف فرعی زیر نیز مدنظر است:

۱. شناسایی عوامل تاثیرگذار و تاثیرپذیر از استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ در اجرای سامانه مدیریت دانش

۲. شناسایی عوامل موثر از استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ در اجرای سامانه مدیریت دانش از منظر محرمانگی، یکپارچگی و دسترس پذیربودن اطلاعات

در ارتباط با اهداف فوق سوال اصلی پژوهش این است که تاثیر امنیت فن‌آوری اطلاعات براساس استاندارد ISO/IEC ۲۷۰۰۱:۲۰۱۳ در اجرای سامانه مدیریت دانش چگونه است؟

همچنین، سوال‌های فرعی زیر نیز مطرح است:

۱. اهداف کنترلی تاثیرگذار و تاثیرپذیر از استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ در اجرای سامانه مدیریت دانش کدام‌اند؟
۲. مهم‌ترین اهداف کنترلی استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ در اجرای سامانه مدیریت دانش از منظر محرمانگی، یکپارچگی و دسترس پذیربودن اطلاعات کدامند؟

بی‌گمان، موارد ذیل حاکی از اهمیت و ضرورت انجام این پژوهش است:

۱. تبیین آثار استقرار استاندارد ISO/IEC ۲۷۰۰۱:۲۰۱۳ در استقرار سامانه مدیریت دانش
۲. افزایش حمایت و سرمایه‌گذاری برای ارتقاء زیرساخت‌های فناوری اطلاعات برای اجرای امن سامانه مدیریت دانش
۳. کاهش دغدغه‌های امنیت اطلاعات در اجرای سامانه مدیریت دانش

براساس بررسی‌هایی که تاکنون به‌عمل آمده است، پژوهشی با عنوان تاثیر امنیت فناوری اطلاعات طبق استاندارد ISO/IEC ۲۷۰۰۱:۲۰۱۳ بر اجرای سامانه نرم‌افزاری مدیریت دانش در سازمان‌های نظامی ایران مشاهده نگردید، بنابراین، باتوجه به جستجوهای انجام شده به‌نظر می‌رسد در این خصوص تحقیقات کمی صورت گرفته است.

۲- مبانی نظری و پیشینه پژوهش

حدود ۲۱ درصد از کل نواقص شناسایی شده در سازمان‌های مورد ارزیابی، مربوط به امنیت اطلاعات بوده است. مهم‌ترین دلیل آن این است که کنترل‌های امنیتی کافی در سازمان‌های مورد مطالعه وجود نداشتند و در سازمان‌هایی هم که وجود داشتند، به‌صورت موثری به‌کار گرفته نمی‌شدند[۱۰]. امروزه بیشترین چالش‌های امنیت اطلاعات در استفاده از ابزارها و فن‌آوری‌های امنیت از قبیل رمزنگاری، فایروال‌ها، مدیریت دسترسی‌ها و سایر مواردی از این قبیل روی می‌دهند[۱۸]. اگرچه ابزار و فن‌آوری‌ها جزیی جدایی‌ناپذیر از طرح‌های امنیت اطلاعات سازمان هستند، بحث بر سر این است که آن‌ها به‌تنهایی برای حل مشکلات امنیت اطلاعات کافی نیستند[۱۴]. برای بهبود کلی امنیت اطلاعات، سازمان‌ها باید

کنترل‌های مناسبی که نیازمندی‌های امنیتی خاص آن‌ها را برآورده می‌کند، ارزیابی و پیاده‌سازی نمایند[۱۲]. به‌دلیل تنوع محدودیت‌های خاص هر سازمان (برای مثال هزینه‌ها، منابع در دسترس)، سازمان‌ها از موهبت انتخاب و پیاده‌سازی تمام کنترل‌های امنیت اطلاعات برخوردار نیستند[۱۵]. ارزیابی کافی از کنترل‌های امنیت اطلاعات برای بقای سازمان‌ها از منظر امنیت اطلاعات به اندازه محافظت از دارایی‌های اطلاعات مالی آن‌ها حیاتی است. با این وجود، بررسی سوابق موضوعات، شکاف‌ها و یا نقاط ضعفی را مشخص می‌سازند که روش‌های ارزیابی امنیت اطلاعات سنتی از کنترل‌های امنیت اطلاعات به‌صورت موثر و اثربخش در سازمان ممانعت به‌عمل می‌آورند. این نقاط ضعف مشخص شده در سوابق نه‌تنها بر فرایند انتخاب کنترل‌های امنیت اطلاعات تاثیرگذار است، همچنین محافظت کلی از محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات را نیز تحت تاثیر قرار می‌دهد[۱۷]. در ادامه به بررسی تعدادی از رویکردها و روش‌های به‌کارگرفته شده در سازمان‌ها، به همراه برخی از نقاط ضعف آن‌ها خواهیم پرداخت:

۲-۱- تجزیه و تحلیل و مدیریت ریسک

نتیجه انجام تجزیه و تحلیل و مدیریت ریسک، ارایه فهرستی از نیازمندی‌های امنیت اطلاعات است، به صورتی‌که کنترل‌های امنیت اطلاعات برای کاهش مخاطرات پیشنهاد داده می‌شود[۸]. تجزیه و تحلیل و مدیریت ریسک، رویکردی پایین به بالا است، که محدودیت‌های خاص سازمان‌ها را در نظر نمی‌گیرد[۱۹]. تجزیه و تحلیل و مدیریت ریسک به‌عنوان بهترین یا اساسی‌ترین ابزار برای اطمینان از امنیت اطلاعات نیست. سازمان‌ها، هنگام انجام تجزیه و تحلیل و مدیریت ریسک، کنترل‌هایی را به‌کار می‌گیرند که غیرضروری و یا بی‌اهمیت هستند. علاوه بر این، اتکای صرف بر تجزیه و تحلیل و مدیریت ریسک، اغلب مورد انتقاد است، زیرا اثبات گردیده که حداکثر نمودن امنیت اطلاعات با درنظر گرفتن منافع مالی، مسئله‌ای غامض و دشوار است[۱۳].

۲-۲- راهنماهای پایه یا چارچوب‌های نمونه، رویکردهای موقت

برخی از بهترین نمونه‌های کاربردی عبارت‌اند از: اهداف کنترلی برای اطلاعات و فناوری‌های مرتبط[۱]، کتاب‌خانه زیرساخت فناوری اطلاعات[۲]، چارچوب موسسه بین‌المللی استاندارد و فن‌آوری[۳]، ایزو ۲۷۰۰۲، ایزو ۲۷۰۰۱، ایزو ۱۷۷۹۹، مدل بلوغ توانایی‌ها[۴] و معماری امنیت اطلاعات[۵]. فرایند انتخاب موثرترین کنترل‌های امنیت اطلاعات از راهنماهای پایه یا بهترین نمونه‌های کاربردی چالش دیگری است[۱۲]. راهنماهای پایه یا بهترین نمونه‌های کاربردی به کاربر در انتخاب کنترل امنیت اطلاعات کمک می‌کنند،

---

۱. COBIT
۲. ITIL
۳. NIST
۴. CMM
۵. ISA

اما راهنمایی کمی در انتخاب بهترین کنترل‌ها با درنظر گرفتن محدودیت‌های خاصی مانند هزینه‌ها، برنامه زمان‌بندی و محدودیت منابع ارائه می‌کنند[۱۹]. سایر روش‌های غیر رسمی‌تر، مانند رویکردهای موقت یا تصادفی، نیز ممکن است منجر به انتخاب کنترل‌های امنیت اطلاعات غیرضروری منجر گردند[۸].

۲-۳- چک‌لیست‌های امنیت اطلاعات

چن و یون، چک‌لیست‌هایی را برای شناسایی کنترل‌های امنیت اطلاعات متعارف، شامل ریسک‌های امنیت اطلاعات در سازمان‌های مبتنی بر رایانش ابری به‌کار بردند[۱۱]. اهمیت آن‌ها در شناسایی تمامی تهدیدات متصور بر یک سیستم رایانه‌ای و پیشنهاد راه‌کارهای مقابله با تهدیدات است[۱۳]. با این وجود، دیلن و ترک‌زاده، تاکید دارند در طی زمان، اهمیت آن‌ها کاهش خواهد یافت، زیرا اطلاعات کمی با درنظر گرفتن این نوع تحلیل ایستا فراهم می‌گردد. اگرچه چک‌لیست‌ها ممکن است ابزار خوبی برای اطمینان از امنیت اطلاعات درنظر گرفته شوند، اما اتکاء صرف بر آن‌ها منجر به ایجاد استراتژی‌های امنیتی ضعیف در سیستم‌های اطلاعاتی می‌گردد. علاوه براین، چک‌لیست‌ها به‌صورت کامل امور کلیدی برای پاسخ‌گویی به سوال‌های اساسی را پوشش نمی‌دهند[۷]. چک‌لیست‌ها بدون انجام هرگونه تحلیل مستمر در ارتباط با نوع اقدامات شناسایی شده، فقط بر آن چیزی که می‌توان انجام داد، متمرکز شده است[۹].

۲-٤- فرآیند انتخاب کنترل

برنارد و وون سلمز، فرآیند انتخاب کنترل را برای ارزیابی کنترل‌های امنیت اطلاعات رسمیت بخشیدند، فرآیندی که نیاز به انتخاب تصادفی/غیرضروری، را حذف می‌کند؛ همچنان‌که در استاندارد انگلیسی BS۷۷۹۹ سیاست‌های امنیت اطلاعات برای شناسایی کنترل‌های امنیت اطلاعات یکپارچه گردیده‌اند. تجزیه و تحلیل کسب و کار شامل مجموعه‌ای از سوال‌های است که شرایط خاص کسب وکار را تجزیه و تحلیل نموده، میزان اهمیت امنیت و مدیریت امنیت اطلاعات را برای سازمان مشخص می‌نماید. اقدامات فوق سیاست‌های امنیت اطلاعات خاصی را برای سازمان پیشنهاد می‌دهد.

این سیاست‌ها به‌وسیله یک یا چند مورد از کنترل‌های امنیت اطلاعات BS۷۷۹۹، الزامی شده است. برنارد و وون سلمز، استدلال نمودند که رویکرد پیشنهادی آن‌ها در مورد فرآیند انتخاب کنترل از طریق تجزیه و تحلیل کسب و کار جاری که منجر به تعیین نیازمندی‌های امنیت و سیاست‌های امنیت اطلاعات می‌گردد، برای مشخص نمودن کنترل‌های امنیت اطلاعات ضروری است[۸]. این فرآیند دربرگیرنده‌ی درجه بالایی از برداشت فردی برای انتخاب کنترل‌های امنیت اطلاعات است[۱۵].

۲-۵- سیستم مدیریت امنیت اطلاعات

سیستم مدیریت امنیت اطلاعات، بخشی از سیستم‌های مدیریتی سازمان است که بر پایه رویکرد مخاطرات سازمان قرار داشته و هدف از آن پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی، نگهداری و بهبود امنیت اطلاعات است. این سیستم رویکردی تحولی در مدیریت سازمان است و سعی دارد امنیتی سازمان‌یافته، سیستماتیک و یکپارچه ایجاد نماید و با یک دیدگاه کلان‌نگر و بالا به پایین با ارایه یک روش‌شناسی رسمی، گام به گام آن را در سازمان اجرا نماید[۳].

در پژوهشی که توسط شفقتی و پیله‌وری برای شناسایی عوامل مدیریتی موثر بر امنیت اطلاعات در دانشگاه علوم پزشکی تهران انجام شده است، برای تصمیم‌گیری گروهی، روش فازی و برای مدل‌سازی مقادیر زبانی و غیرقطعی در نظریه‌ها، از تئوری فازی استفاده کرده‌اند تا بااستفاده از آن‌ها مهم‌ترین شاخصه‌های مدیریتی موثر بر امنیت سازمان شناسایی گردند. سپس، با استفـاده از روش وایکر[۱]، شاخص‌های حاصل از روش دلفی فازی، اولویت‌بندی شدند[۱۶]. یانگ، شی‌یه و تزنگ، مدل ترکیبی دیمتل، فرایند تحلیل شبکه و وایکور را برای حل مسائل حاوی معیارهای پیچیده که بین آن‌ها وابستگی و بازخورد وجود دارد را برای ارزیابی و کنترل ریسک امنیت اطلاعات به‌کار بردند[۲۰].

۳- شمایی از سامانه مدیریت دانش

سامانه مدیریت دانش، مدیران را در راستای پیشبرد نظام دانشی یاری می‌کند و با اتوماسیون رویه‌ها به کارکنان این امکان را می‌دهد تا با فراغت بال بیشتر و دور از بوروکراسی‌های معمول اداری، دانش خود را به سازمان ارائه و از دانش سایر افراد بهره‌برداری کنند. ویژگی‌های اصلی این سامانه به این‌شرح است: استقرار نظام مستندسازی، تهیه نسخه پشتیبان از اسناد و مدارک حیاتی پروژه‌ها، ترسیم نقشه دانش، بانک تخصصی خبرگان، طراحی مکانیزم انگیزشی برای محققان سازمان در تولید و تسهیم دانش، طراحی مکانیزم شناسایی و اکتساب دانش‌های ضمنی بازنشستگان و کارکنان کلیدی درحال رهایی، طراحی مکانیزم ارزیابی و ارزش‌گذاری دانش‌های سازمان، طراحی مکانیزم رتبه‌بندی دانش‌گران سازمان براساس عملکرد دانشی و حمایت از حق مالکیت معنوی دانش‌گران، ایجاد پایگاه دانش، ارایه گزارش های متنوع مدیریتی از عملکرد دانشی کارکنان. همچنین، این سامانه برای غلبه بر مشکلات زیر، سازمان را یاری می‌کند:

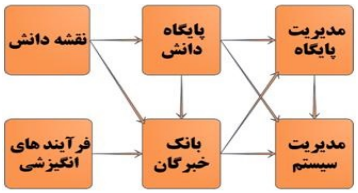
- پیدا نکردن اطلاعاتی که برای تهیه آن‌ها هزینه یا زمان قابل توجهی صرف شده است.
- دسترسی نداشتن به دانش‌هایی که بخشی از دارایی سازمان به شمار می‌آیند(در زمان مناسب و با کیفیت مطلوب).

---

۱. VIKOR

- رفتن نیروهای کلیدی از سازمان و از بین رفتن دانش و تجربه ذهنی آن‌ها
- صرف هزینه‌های مکرر برای انتقال و اشتراک دانش بین افراد
- ناتوانی در مدیریت مناسب بر روی دانش‌ها و اطلاعات محرمانه

این سامانه از پنج بخش اصلی مطابق شکل ۱، تشکیل شده است.

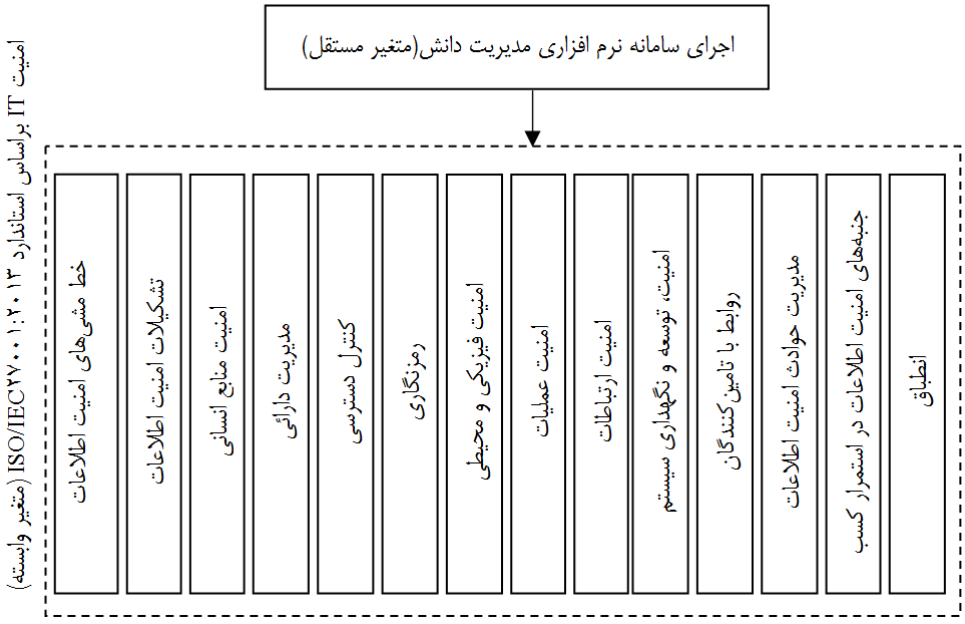


شکل ۱- بخش‌های مختلف سامانه مدیریت دانش

پراکندگی جغرافیایی، تعدد مراکز صنعتی و تحقیقاتی برخی سازمان‌ها، کافی نبودن و یا استفاده نکردن از بسترهای ایجاد شده توسط فناوری اطلاعات و بسیاری مسائل دیگر از این قبیل، به دلیل دغدغه‌های ناشی از امنیت فن‌آوری اطلاعات، استقرار سامانه مدیریت دانش را با مشکل مواجه می‌کند. فن‌آوری اطلاعات در ایجاد نقشه دانش و فن‌آوری، تهیه بانک خبرگان، ثبت و گردش مستندات علمی و فنی، ثبت و انتشار درس آموخته‌های پروژه و بسیاری از مسایل حوزه تحقیق و توسعه در یک قالب یکپارچه می‌تواند نقش موثری داشته باشد. اگرچه برخی سازمان‌ها با تدوین چک لیست‌های متفاوت و ممیزی حوزه فن‌آوری اطلاعات براساس آن‌ها سعی در ارتقای سطح امنیت فن‌آوری اطلاعات دارند، اما این اقدامات شاید نتواند به‌عنوان یک سیستم منسجم و یکپارچه، نظرات مساعد درخصوص ایجاد امنیتی پایدار را جلب و تمام ابعاد مربوط را بررسی نماید. پژوهش حاضر تاثیر استاندارد ISO/IEC ۲۷۰۰۱:۲۰۱۳ را در استقرار امن سامانه مدیریت دانش بررسی خواهد کرد.

٤- مدل مفهومی پژوهش

باتوجه به مطالعات انجام شده، چارچوب مفهومی تحقیق به‌صورت شکل ۲ منظور شده است:



شکل ۲- چارچوب مفهومی تحقیق

٤-۱- فرضیه‌های پژوهش

فرضیه اصلی: امنیت فن‌آوری اطلاعات براساس استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ در اجرای سامانه مدیریت دانش، تاثیر دارد.

فرضیه‌های فرعی:

۱. اهداف کنترلی A۱۷, A۱٦, A۱۳, A۱۲, A۱۱, A۱۰, A٦ (طبق جدول۲) بر سایر اهداف کنترلی استاندارد ISO/IEC۲۷۰۰۱ در اجرای سامانه مدیریت دانش اثرگذارند.
۲. اهداف کنترلی استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ (طبق جدول۲) در اجرای سامانه مدیریت دانش از منظر محرمانگی، یکپارچگی و دسترس‌پذیربودن اطلاعات تاثیر یکسانی ندارند.

۵- روش تحقیق

پژوهش حاضر از نظر روش از نوع تحقیق توصیفی-پیمایشی و از نظر هدف کاربردی است. برای گردآوری داده‌ها، از روش کتابخانه‌ای، جستجوی اینترنتی و استفاده از سایت‌های علمی اینترنتی(مانند ... ,Science direct, Emerald) بهره برده شده است. قلمرو موضوعی، نقش امنیت فن‌آوری اطلاعات براساس استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ در استقرار سامانه نرم‌افزاری مدیریت دانش است. متغیرهای این پژوهش عبارت‌اند از:

متغیر مستقل، شامل؛ اجرای سامانه نرم‌افزاری مدیریت دانش در سازمان

متغیرهای وابسته، شامل؛ اهداف کنترلی امنیت فناوری اطلاعات و ارتباطات بر اساس استاندارد ISO/IEC ۲۷۰۰۱:۲۰۱۳ است.

نظرات خبرگان درزمینه‌ی نقش اهداف کنترلی استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ از سه منظر محرمانگی، یکپارچگی و دسترس‌پذیری بر امنیت سامانه مورد نظر از طریق توزیع پرسش‌نامه استاندارد روش‌های دیمتل و فرآیند تحلیل شبکه‌ای در بین جامعه آماری، جمع‌آوری شده است. دراین پرسش‌نامه از مقیاس ۹ کمیتی طبق جدول ۱ استفاده شده است.

جدول ۱- طیف پنج درجه تکنیک دیمتل و معادل قطعی برای عبارات کلامی[۵]

درجه اهمیت	تعریف	شرح
۱	اهمیت یکسان	دوعنصر اهمیت یکسانی داشته باشند
۳	نسبتا مرجح	یک عنصر نسبت به عنصر دیگر، نسبتا ترجیح داده می‌شود.
۵	ترجیح زیاد	یک عنصر نسبت به عنصر دیگر، زیاد ترجیح داده می‌شود.
۷	ترجیح بسیار زیاد	یک عنصر به عنصر دیگر، بسیار زیاد ترجیح داده می‌شود.
۹	ترجیح فوق‌العاده زیاد	یک عنصر به عنصر دیگر، ترجیح فوق‌العاده زیادی دارد.
۸,۶,۴,۲	ارزش‌های بینابین در قضاوت‌ها	

با استفاده از روش دیمتل، روابط علی و معلولی عناصر مشخص گردیده است و شبکه مرتبط از اهداف کنترلی استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ به‌منظور شناسایی روابط داخلی بین آن‌ها ایجاد و سپس شدت اثر روابط داخلی مشخص گردیده‌اند. همچنین از روش فرایند تحلیل شبکه‌ای برای رتبه‌بندی اهداف کنترلی استفاده شده است. ابتدا ساختار شبکه‌ای موضوع پژوهش تهیه شده است، سپس مقایسات زوجی بین اهداف کنترلی استاندارد فوق برای شناسایی میزان ارتباط آن‌ها با یکدیگر صورت گرفته است.

اهمیت نسبی عناصر محاسبه و سپس ماتریس‌ها، وزن‌دهی و نرمال سازی گردیده‌اند. نتایج حاصل از این مقایسات زوجی سوپرماتریس حدی را تشکیل داده‌اند. برای تایید روایی پرسش‌نامه‌ها تایید ۳ نفر از صاحب‌نظران و خبرگان حوزه امنیت فن‌آوری اطلاعات و آشنا با شرایط سازمان، اخذ شده است. پایایی پرسش‌نامه‌ها از طریق محاسبه نرخ سازگاری ماتریس مقایسات زوجی، مورد بررسی قرار گرفته است. درصورتی‌که نرخ سازگاری کوچک‌تر یا مساوی ۰/۱باشد، در مقایسات زوجی سازگاری وجود دارد و می-توان کار را ادامه داد. این نرخ ناسازگاری برای کلیه مقایسات صورت گرفته کمتر از ۰/۱ است، بر این اساس، پایایی پرسش‌نامه‌ها نیز مورد تایید است.

۶-۲- جامعه آماری

موضوع پژوهش حاضر در حیطه مدیران و کارشناسان فن‌آوری اطلاعات و امنیت فن‌آوری اطلاعات سازمان نظامی مورد نظر است، بر این اساس، این افراد به‌عنوان جامعه آماری در نظر گرفته شده‌اند. تعداد اعضای جامعه ۲۳ نفر است، با توجه به محدود بودن تعداد اعضای جامعه، از همه آن‌ها در پژوهش استفاده گردید.

۶-۳- تعیین عوامل پژوهش

عوامل موجود در این تحقیق شامل چهارده هدف کنترلی استاندارد :ISO/IEC۲۷۰۰۱، به شرح جدول ۲ است. برای آزمون فرضیه‌ها و رتبه‌بندی عوامل موثر بر امنیت سامانه موردنظر تکنیک ترکیبی دیمتل و فرآیند تحلیل شبکه‌ای منظور شده است.

جدول۲- عوامل مورد استفاده در تحقیق

کدشناسایی	هدف کنترلی
A5	خط‌مشی‌های امنیت اطلاعات
A6	تشکیلات امنیت اطلاعات
A7	امنیت منابع انسانی
A8	مدیریت دارایی
A9	کنترل دسترسی
A10	رمزنگاری
A11	امنیت فیزیکی و محیطی
A12	امنیت عملیات
A13	امنیت ارتباطات

A14	امنیت، توسعه و نگهداری سیستم
A15	روابط با تامین‌کنندگان
A16	مدیریت حوادث امنیت اطلاعات
A17	جنبه‌های امنیت اطلاعات در استمرار کسب وکار
A18	انطباق

۶-۴- تعیین روابط حاکم بین عوامل از طریق مقایسات زوجی

ماتریس مقایسات زوجی طبق شکل ۳ میان عوامل که بیانگر میزان تاثیر رابطه بین آن‌ها است، طبق نظر خبرگان تشکیل شده است [۶].

$$Z = \begin{array}{c} \\ c_1 \\ c_2 \\ \vdots \\ c_n \end{array} \begin{array}{c} \begin{array}{cccc} c_1 & c_2 & \cdots & c_n \end{array} \\ \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ a_{21} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & 1 \end{pmatrix} \end{array}$$

شکل۳- ماتریس مقایسات زوجی بین عوامل

باتوجه به ماهیت تصمیم‌گیری گروهی، به‌منظور تهیه نظرات گروهی در قالب یک ماتریس واحد از رابطه۱ استفاده شده است.

رابطه ۱)
$$A_{ij}=\frac{1}{K}\sum_{L=1}^{k} a_{ijl}$$

A_{ij}: درایه‌های ماتریس تجمیع شده، K: حداکثر تعداد نفرات، L: تعداد نفرات

۶-۵- تشکیل ماتریس نرمال‌شده روابط مستقیم

جمع سطری درایه‌های ماتریس N براساس رابطه۲ محاسبه و طبق رابطه۳، معکوس بیشترین آن در درایه‌های ماتریس N ضرب گردیده است تا شدت نسبی حاکم بر روابط مستقیم تعیین گردد.

رابطه ۲)
$$N= \alpha * M$$

رابطه ۳)
$$\alpha = \frac{1}{\mathrm{Max}\sum_{j=1}^{n} a_{ij}}$$

۶-۶- محاسبه ماتریس شدت روابط کل

ماتریس شدت نسبی موجود از روابط مستقیم و غیرمستقیم (T)، با استفاده از رابطه۴ ، به‌دست آورده شده است:

رابطه ۴) $T=N(I-N)^{-1}$

N: ماتریس نرمال بدست آمده از مرحله قبل، **I:** ماتریس واحد

۶-۷- محاسبه فاکتورهای تاثیرگذار، تاثیرپذیر، بردار برتری و بردار ارتباط

فاکتورهای فوق براساس روابط ذیل مشخص گردیده‌اند:

رابطه ۵) $Di=\sum_{j=1}^{n} t_{ij}$ i= ۱،۲، …، n

رابطه ۶) $Rj=\sum_{i=1}^{n} t_{ij}$ j= ۱،۲، …، n

رابطه ۷) بردار برتری :D+R

رابطه ۸) بردار ارتباط :D-R

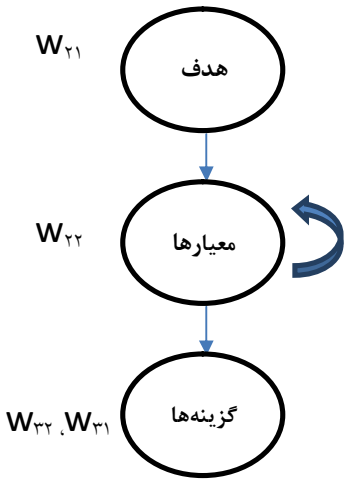
R: جمع سطری درایه‌های ماتریس T برای هریک از عوامل که معرف میزان تاثیرگذاری آن عامل نسبت به سایر عوامل ماتریس است.

D: جمع ستونی درایه‌های ماتریس T برای هر عامل که معرف میزان شدت تاثیرپذیری از سایر عوامل است.

بردار برتری: برداری افقی که مشخص کننده مجموع تاثیرگذاری و تاثیرپذیری عامل موردنظر است. عاملی که بیشترین مقدار R+D را داشته باشد، بیشترین تعامل را با سایر عوامل خواهد داشت.

بردار ارتباط: برداری عمودی که مقدار نهایی تاثیرگذاری هرعامل بر مجموع عناصر دیگر در سیستم را نشان می‌دهد. اگر R>D آن‌گاه R-D>۰ ، بنابراین این عامل یک تاثیرگذار قطعی است و یک متغیر علت(اثرگذار) محسوب می‌شود. اگر R<D آن‌گاه R-D<۰ ، بنابراین عامل یک تاثیرپذیر قطعی است و یک متغیر معلول(اثرپذیر) محسوب می‌شود.

نمودار علی و معلولی در دستگاه مختصات دکارتی براساس زوج مرتب (R+D,R-D) به‌دست می‌آید. بر اساس شکل۴، ساختار ارتباط شبکه‌ای بدین‌صورت تشکیل می‌گردد: وزن نسبی بین معیارها باتوجه به گره هدف، وزن داخلی بین معیارها، وزن زیرمعیارها نسبت به هدف و وزن زیرمعیارها نسبت به معیارها.



شکل٤- ساختار شبکه‌ای

نرمال‌سازی هریک از ماتریس‌های مقایسات زوجی با استفاده از روش پیشنهادی آقای ساعتی طبق رابطهٔ ذیل انجام گرفته است:

رابطه ۹)
$$n_{ij}=\frac{a_{ij}}{\sum_{j=۱}^{m} a_{ij}}$$

محاسبه وزن نسبی ماتریس مقایسات زوجی از روش میانگین حسابی، بااستفاده از رابطهٔ زیر:

رابطه ۱۰)
$$w_{ij}=\frac{۱}{n}\sum_{j=۱}^{n} a_{ij} \qquad i= ۱،۲, \dots , m$$

n تعداد سطر یا ستون در ماتریس مقایسات زوجی است.

محاسبه سازگاری ماتریس مقایسات زوجی به‌شرح ذیل صورت گرفته است:

رابطه ۱۱)
$$D.W=\lambda.W$$

D: ماتریس مقایسات زوجی، W: ماتریس وزن‌دهی، λ: مقدار بردار ویژه

رابطه ۱۲)
$$\lambda.W \div W= \lambda_{max}$$

متوسط λ_{max} طبق رابطه زیر به‌دست آمده است:

رابطه ۱۳)
$$\lambda_{max}=\frac{\sum_{i=۱}^{m} \lambda_i}{n}$$

بااستفاده از رابطه‌ی زیر مقدار شاخص سازگاری بدست آمده است:

رابطه ۱۴)
$$CI=\frac{\lambda_{max}-n}{n-۱}$$

شاخص سازگاری تصادفی(RI) طبق جدول استاندارد ۳ محاسبه شده است:

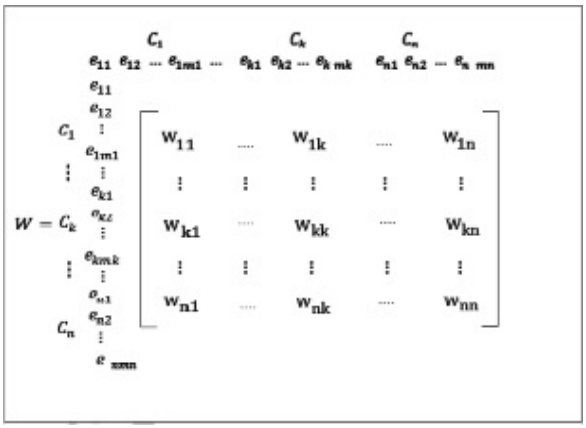
جدول۳- جدول تعیین شاخص سازگاری تصادفی

N	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴
RI	۰	۰	۰/۵۸	۰/۹	۱/۱۲	۱/۲۴	۱/۳۲	۱/۴۱	۱/۴۵	۱/۴۵	۱/۵۱	۱/۴۸	۱/۵۶	۱/۵۷

N تعداد سطرها یا ستون‌های ماتریس است.

۶-۸- تشکیل سوپر ماتریس اولیه، سوپر ماتریس وزنی و ماتریس حدی

تهیه سوپر ماتریس اولیه طبق شکل۵، Cn: نشاندهنده خوشه N اُم، eNn: عنصرn اُم در خوشه N اُم، Wij: ماتریس بلوک شامل وزنهای نسبی بردارهای w تاثیر عناصر در خوشه i اُم نسبت به خوشه j است. اگر خوشه i هیچ تأثیری بر خوشه i اُم خودش نداشته باشد (حالت وابستگی داخلی) Wij ، صفرمی‌شود.



شکل ۵- ساختار سوپرماتریس

درواقع، ستون‌های سوپرماتریس اولیه از چند بردار ویژه تشکیل می‌گردد که جمع هرکدام از بردارها برابر یک است. بنابراین این امکان وجود دارد که جمع هر ستون سوپرماتریس اولیه بیش از یک باشد. برای آن‌که از عناصر ستون متناسب با وزن نسبیشان فاکتور گرفته شود و جمع ستون برابریک شود، هر ستون ماتریس، استاندارد شده است تا جمع هریک از ستون‌های آن برابر یک گردد. سوپرماتریس وزنی، به

توان حدی می‌رسد تا عناصر ماتریس همگرا و مقادیر سطری آن باهم برابر گردند.
براساس ماتریس به‌دست آمده، بردار وزن عمومی مشخص می‌گردد.

رابطه ۱۶) $\lim_{k\to\infty} w^k$

ماتریسی که در نتیجه به توان رسیدن ماتریس وزنی به‌دست می‌آید، ماتریسی حدی است که مقادیر هر سطر آن با هم برابر است.

٦- تجزیه و تحلیل داده‌ها

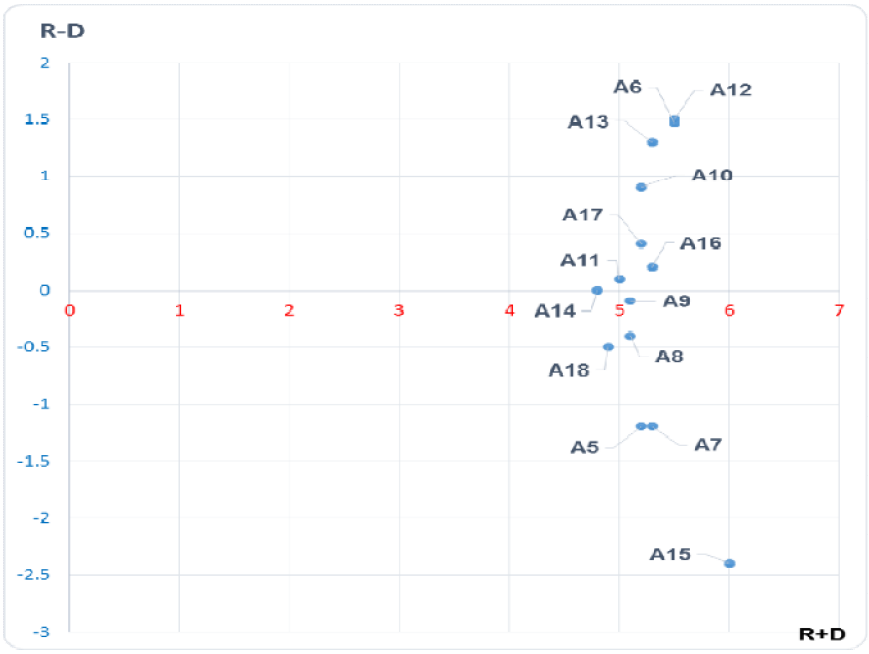
میزان تاثیرگذاری، تاثیر پذیری و مولفه‌های ترسیم نمودار علی– معلولی حاصل از ماتریسT طبق جدول۴، حاصل شده است.

جدول٤- محاسبه بردار برتری و بردار ارتباط برای هر عامل

هدف کنترلی	R	D	R+D	R-D
A5	۲	۳/۱۹	۵/۱۹	-۱/۱۹
A6	۳/۵۱	۲/۰۱	۵/۵۲	۱/۴۷
A7	۲/۰۴	۳/۲۶	۵/۳	-۱/۲۲
A8	۲/۳۸	۲/۷۸	۵/۱۶	-۰/۴
A9	۲/۴۹	۲/۵۸	۵/۰۷	-۰/۰۹
A10	۳/۰۳	۲/۱۹	۵/۲۲	۰/۸۴
A11	۲/۵۲	۲/۴۷	۴/۹۹	۰/۰۵
A12	۳/۴۸	۱/۹۸	۵/۴۶	۱/۵
A13	۳/۳۱	۱/۹۷	۵/۲۸	۱/۳۴
A14	۲/۴۱	۲/۴۲	۴/۸۲	-۰/۰۱
A15	۱/۷۷	۴/۲	۵/۹۷	-۲/۴۳
A16	۲/۷۴	۲/۶	۵/۳۴	۰/۱۴
A17	۲/۸۳	۲/۴	۵/۲۳	۰/۴۳
A18	۲/۱۹	۲/۶۶	۴/۸۵	-۰/۴۷

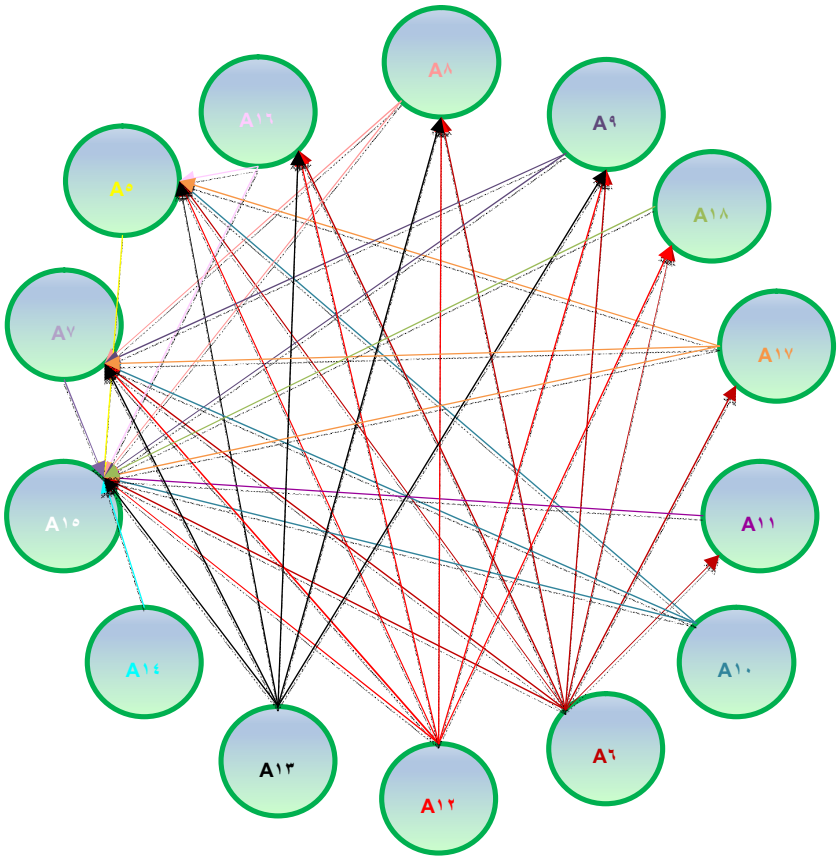
نمودار علی- معلولی

نمودار شکل۶، براساس زوج مرتب‌های (R+D,R-D)، ترسیم شده است. به کمک این نمودار متغیرهای علت و معلول، رتبه‌بندی میزان تاثیرگذاری و میزان اهمیت اهداف کنترلی مشخص می‌گردند.



شکل ٦- نمودار علی و معلولی عوامل

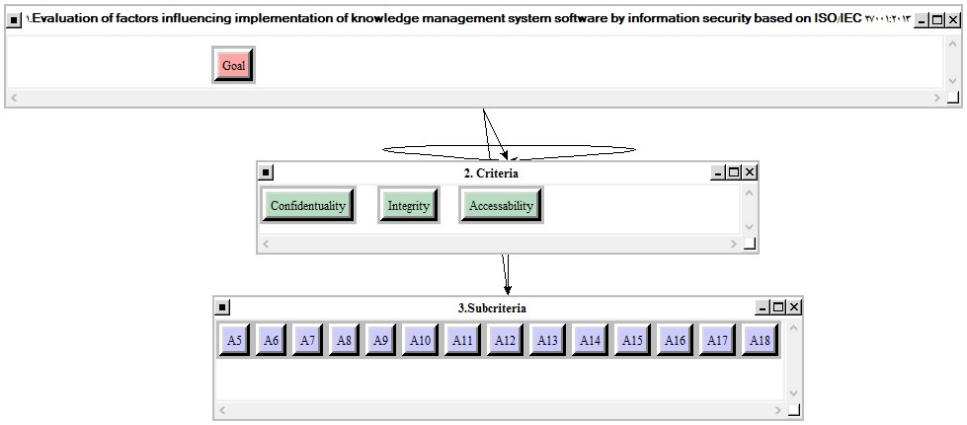
با محاسبه ارزش آستانه روابط از طریق محاسبه میانگین مقادیر ماتریس روابط کل، از روابط جزئی(تمامی روابط با مقدار کوچک‌تر از مقدار آستانه در ماتریس روابط کل)صرف‌نظر شده است. در این پژوهش مقدار میانگین مقادیر ماتریس روابط کل برابر ۰,۱۹ است، اما باتوجه به مذاکره با خبرگان، مقدار آستانه برابر ۰/۲۳درنظر گرفته شد و نقشه روابط شبکه مطابق شکل۷، به‌دست آمده است.



شکل ۷- نقشه روابط شبکه

ساختار شبکه‌ای

ساختار شبکه‌ای پژوهش بااستفاده از نرم‌افزار SuperDecision مطابق شکل۸ است.



شکل ۸- ساختار شبکه‌ای پژوهش

مقایسه زوجی معیارها با یکدیگر

اعضای پنل خبرگان به اتفاق تاکید براثرگذاری سه معیار محرمانگی، یکپارچگی و دسترس‌پذیری بر یکدیگر به‌صورت یکسان بر مقوله امنیت اطلاعات داشتند. میزان سازگاری مقایسات برابر صفر و کمتر از مقدار آستانه ۰/۱ است، بر این اساس، مقایسات قابل پذیرش است.

مقایسه اهداف کنترلی ۱۴گانه استاندارد ISO/IEC ۲۷۰۰۱:۲۰۱۳ به‌عنوان زیرمعیارها با درنظر گرفتن نقش آن‌ها در استقرار سامانه مدیریت دانش و با درنظر گرفتن ماتریس شدت روابط مستقیم حاصل از روش دیمتل و باتوجه به مقدار آستانه منظور شده است. سازگاری مقایسات برابر ۰/۰۴ و بر این اساس، قابل پذیرش است.

سازگاری مقایسات زوجی انجام شده برای اهداف کنترلی ۱۴گانه استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ باتوجه به معیارهای محرمانگی، یکپارچگی و دسترس‌پذیری، کمتر از ۰/۱ و بر این اساس، مورد پذیرش هستند.

باتوجه به مقایسات زوجی صورت گرفته فوق، سوپرماتریس اولیه یا ناموزون برابر جدول ۵ حاصل شده است.

جدول ۵- سوپرماتریس اولیه

		1.GOAL	2. Criteria			3.Subcriteria
		Goal	A	C	I	A5-A18
1.G	Goal	۰	۰	۰	۰	
2. C	A	۰/۳۳	۰/۳۳	۰/۳۳	۰/۳۳	
	C	۰/۳۳	۰/۳۳	۰/۳۳	۰/۳۳	
	I	۰/۳۳	۰/۳۳	۰/۳۳	۰/۳۳	
3.S	A5	۰/۱۲۳	۰/۰۲۹	۰/۰۴۴	۰/۰۳۹	
	A6	۰/۰۲۶	۰/۱۳۹	۰/۱۵۷	۰/۱۵۳	
	A7	۰/۱۱۹	۰/۰۴۲	۰/۰۴۷	۰/۰۵	
	A8	۰/۰۷۶	۰/۰۵۵	۰/۰۴۴	۰/۰۴۵	
	A9	۰/۰۷۲	۰/۰۶۲	۰/۰۷۲	۰/۰۷۲	
	A10	۰/۰۳۵	۰/۱	۰/۰۹۸	۰/۰۹۱	۰
	A11	۰/۰۵۸	۰/۰۵۲	۰/۰۵۵	۰/۰۵۵	
	A12	۰/۰۲۹	۰/۱۸۴	۰/۱۳۵	۰/۱۳۵	
	A13	۰/۰۲۹	۰/۱۳۵	۰/۱۱۴	۰/۱۱۷	
	A14	۰/۰۳۶	۰/۰۶۹	۰/۰۸	۰/۰۸	
	A15	۰/۲	۰/۰۱۳	۰/۰۱۵	۰/۰۱۴	
	A16	۰/۰۷۴	۰/۰۳۹	۰/۰۴۶	۰/۰۴۶	
	A17	۰/۰۴۹	۰/۰۴۷	۰/۰۵۷	۰/۰۵۸	
	A18	۰/۰۷۳	۰/۰۳۱	۰/۰۳۸	۰/۰۴۳	

وزن نهایی معیارها براساس سوپرماتریس وزنی، برابر جدول۶ ، مشخص شده است.

جدول٦- سوپرماتریس حدی

		1.GOAL	2. Criteria			3.Subcriteria
		Goal	A	C	I	A5 – A18
1.G	Goal	۰	۰	۰	۰	
2. C	A	۰/۱۶۷	۰/۱۶۷	۰/۱۶۷	۰/۱۶۷	
	C	۰/۱۶۷	۰/۱۶۷	۰/۱۶۷	۰/۱۶۷	
	I	۰/۱۶۷	۰/۱۶۷	۰/۱۶۷	۰/۱۶۷	
3.S	A5	۰/۰۱۹	۰/۰۱۹	۰/۰۱۹	۰/۰۱۹	
	A6	۰/۰۷۵	۰/۰۷۵	۰/۰۷۵	۰/۰۷۵	
	A7	۰/۰۲۳	۰/۰۲۳	۰/۰۲۳	۰/۰۲۳	
	A8	۰/۰۲۴	۰/۰۲۴	۰/۰۲۴	۰/۰۲۴	
	A9	۰/۰۳۴	۰/۰۳۴	۰/۰۳۴	۰/۰۳۴	
	A10	۰/۰۴۸	۰/۰۴۸	۰/۰۴۸	۰/۰۴۸	
	A11	۰/۰۲۷	۰/۰۲۷	۰/۰۲۷	۰/۰۲۷	
	A12	۰/۰۷۶	۰/۰۷۶	۰/۰۷۶	۰/۰۷۶	
	A13	۰/۰۶۱	۰/۰۶۱	۰/۰۶۱	۰/۰۶۱	
	A14	۰/۰۳۸	۰/۰۳۸	۰/۰۳۸	۰/۰۳۸	
	A15	۰/۰۰۷	۰/۰۰۷	۰/۰۰۷	۰/۰۰۷	
	A16	۰/۰۲۲	۰/۰۲۲	۰/۰۲۲	۰/۰۲۲	
	A17	۰/۰۲۷	۰/۰۲۷	۰/۰۲۷	۰/۰۲۷	
	A18	۰/۰۱۹	۰/۰۱۹	۰/۰۱۹	۰/۰۱۹	

۷- یافته‌های تحقیق

داده‌های جدول۴، بیانگر این است که عامل A۱۵ دارای بیشترین اهمیت، عوامل A۱۲ وA٦ با فاصله‌ای نزدیک به هم، تاثیرگذارترین عوامل و عامل A۱۵ تاثیرپذیرترین عامل می‌باشد. همچنین پاسخ سوال اول پژوهش بدین‌صورت است: A۱۷, A۱٦, A۱۳, A۱۲, A۱۱, A۱۰, A٦ اهداف کنترلی تاثیرگذار و A۱۸, A۱۵, A۱٤, A۹, A۸, A۷, A۵ به‌عنوان اهداف کنترلی تاثیرپذیر شناسایی شده‌اند.

نمودار شکل۶، نشان می‌دهد که عامل‌های A۱۷, A۱٦, A۱۳, A۱۲, A۱۱, A۱۰, A٦ علی و متغیر علت هستند و عامل‌های A۱۸, A۱۵, A۱٤, A۹, A۸, A۷, A۵ متغیر معلول محسوب می‌گردند، لذا فرضیه اول پژوهش مورد پذیرش قرار می‌گیرد. همچنین اهداف کنترلی به‌ترتیب افزایش تاثیرگذاری(از چپ به راست) به‌شرح ذیل هستند:

A۱۵, A۷, A۵, A۱۸, A۸, A۹, A۱٤, A۱۱, A۱٦, A۱۷, A۱۰, A۱۳, A٦, A۱۲

همان‌طور که در این نمودار نیز مشخص است، از نظر اهمیت، اهداف کنترلی در فاصله‌ای نزدیک به هم قرار دارند و از آن‌جا که برای اخذ گواهینامه ISO/IEC۲۷۰۰۱ می‌بایست کلیه اهداف کنترلی مدنظر قرار گیرند، می‌توان ادعا کرد نتیجه پژوهش با این موضوع هماهنگی دارد.

همان‌طور که در شکل۷ مشاهده می‌گردد اهداف کنترلی A٦, A۱۲, A۱۳, A۱۰ به‌عنوان عواملی هستند که بر اکثر عوامل دیگر تاثیرگذارند و اهداف کنترلی A۵, A۱۵, A۷ عواملی هستند که بیشترین اثرپذیری را از عوامل دیگر دارند. سایر اهداف کنترلی اثرگذاری یا اثرپذیری کمتری نسبت به این عوامل دارند.

بررسی داده‌های حاصل از سوپرماتریس اولیه یا ناموزون بیانگر یکسان نبودن اثرگذاری اهداف کنترلی استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ در اجرای سامانه مدیریت دانش از منظر محرمانگی، یکپارچگی و دسترس پذیربودن اطلاعات است. بنابراین، فرضیه دوم پژوهش تایید می‌گردد. درمورد سوال دوم پژوهش، درمورد معیارهای محرمانگی و یکپارچگی به‌ترتیب اهداف کنترلی A٦، A۱۲، A۱۳ و A۱۰ بیشتر از سایر اهداف کنترلی اولویت دارند و برای معیار دسترس‌پذیری به‌ترتیب اهداف کنترلی A۱۲، A٦، A۱۳ و A۱۰ بیش از سایر اهداف اولویت دارند.

اولویت‌بندی عوامل موثر امنیت اطلاعات براساس استاندارد ISO/IEC ۲۷۰۰۱:۲۰۱۳ در اجرای سامانه نرم‌افزاری مدیریت دانش که در سوال اصلی پژوهش مطرح گردیده، براساس نتایج حاصل از سوپرماتریس حدی به‌شرح زیر است:

A۱۲>A٦>A۱۳>A۱۰>A۱٤>A۹>A۱۱,A۱۷>A۸>A۷>A۱٦>A۵,A۱۸>A۱۵

یافته‌های پژوهش براساس سوپرماتریس حدی بیانگر آن است که اهداف کنترلی استاندارد

ISO/IEC۲۷۰۰۱:۲۰۱۳ بر اجرای امن سامانه نرم‌افزاری مدیریت دانش تاثیر دارد. "امنیت عملیات" بیشترین تاثیر و "روابط با تامین‌کنندگان" کمترین تاثیر را دارد، لذا فرضیه اصلی تحقیق، تایید می‌گردد.

۸- نتیجه‌گیری و پیشنهادهای پژوهش

در این پژوهش، آثار استقرار استاندارد ISO/IEC ۲۷۰۰۱:۲۰۱۳ در پیاده‌سازی امن سامانه مدیریت دانش بررسی شده است. ازنظر خبرگان، اهداف کنترلی A٦ (تشکیلات امنیت اطلاعات)، A۱۲ (امنیت عملیات)، A۱۳ (امنیت ارتباطات) و A۱۰ (رمزنگاری) برتری بیشتری نسبت به سایر اهداف کنترلی استاندارد مذکور در اجرای امن سامانه مدیریت دانش دارند. باتوجه به فقدان ساختارسازمانی مناسب و مستقل برای امنیت اطلاعات در حوزه فن‌آوری اطلاعات و ارتباطات، نبودن مراکزی برای کنترل شبکه و امنیت شبکه و دراختیار نبودن الگوریتم‌های رمزنگاری بومی مناسب، این موضوع قابل تبیین است. استقرار استاندارد مذکور در جلب نظر مساعد مدیران ارشد برای اجرای سامانه مدیریت دانش کارگشا خواهد بود. نتایج پژوهش نشان می‌دهد که: احیاناً با اجرای عوامل اثرگذار بر امنیت سامانه مدیریت دانش، اجرای اهداف کنترلی اثرپذیر آسان‌تر و سریع‌تر خواهد بود. با تکرار پژوهش حاضر، برای سایر دارایی‌ها، شاید بتوان ادعا کرد که نتایج حاصل از آن‌ها نقشه راهی را برای اجرای اهداف کنترلی استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳ در چارچوب برنامه استراتژیک فن‌آوری اطلاعات، ارایه خواهد داد. درصورتی‌که سازمانی برای استقرار ISO/IEC۲۷۰۰۱ با محدودیت منابع روبرو باشد، اولویت‌بندی حاصل برای اهداف کنترلی، می‌تواند مرجعی برای اولویت‌بندی تخصیص منابع، برای تصمیم‌گیران باشد.

پژوهش حاضر از این نظر که فقط در یک سازمان نظامی انجام شده است و سایر سازمان‌ها و شرکت‌ها رادر نظر نگرفته است، با محدودیت مواجه بوده است. ضمنا برای تحقیقات آتی موارد ذیل پیشنهاد می‌گردد:

۱. انجام پژوهش حاضر با استفاده از روش ترکیبی دیمتل و ANP فازی
۲. انجام پژوهش حاضر با درنظر گرفتن ۳۵ سرفصل کنترلی و ۱۱۴ کنترل مذکور در استاندارد ISO/IEC۲۷۰۰۱:۲۰۱۳
۳. انجام پژوهش حاضر برای سایر دارایی‌های سازمان

منابع : **References:**

۱. حسن پور، اکبر، یوسفی زنوز، رضا، موسوی، پریسا (۱۳۹۴). «شناسایی ریسکهای امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری»، مدیریت فناوری اطلاعات، ۷(۱)، تهران، ۱۶۳-۱۸۴.

۲. سرایی، سعیده، هندی، فاطمه (۱۳۹۲). «نقش فناوری اطلاعات در مدیریت دانش»، کنگره ملی مهندسی برق، کامپیوتر و فناوری اطلاعات، مشهد.

۳. صدرعاملی، فریبا، ترک لادانی، بهروز، فراهی، احمد (۱۳۸۸). «تحلیل چالش ها و عوامل موفقیت پیاده سازی سیستم مدیریت امنیت اطلاعات در ایران با استفاده از روش تحلیل سلسله مراتبی»، ششمین کنفرانس بین المللی مدیریت فناوری اطلاعات و ارتباطات، تهران.

۴. کاظمی، مهدی، مذهبی، محمدباقر (۱۳۹۳). «فناوری اطلاعات و بهینه سازی مدیریت دانش»، همایش ملی مهندسی رایانه و مدیریت فناوری اطلاعات، تهران.

۵. مومنی، منصور (۱۳۸۵). «مباحث نوین تحقیق در عملیات»، تهران، انتشارات دانشگاه تهران.

۶. نقاده، حمیده، بیجاری، افسانه (۱۳۹۱)، «اسلایدهای آموزش تکنیک دیمتل»، دسترسی در ۱۳۹۴/۱۰/۲۰ از وب‌سایت: http://www.parsmodir.com/thesis/dematel۲.php.

۷. Backhouse, J. & Dhillon, G. (1996). “Structures of responsibility and security of information systems”. Eur J Inf Syst, 5(1), 2–9.

۸. Barnard, L. & Von Solms, R. (2000). “A formalized approach to the effective selection and evaluation of information security controls”. J Comput Secur, 19(2), 185–194.

۹. Baskerville, R. (1993). “Information systems security design methods: implications for information systems development”. ACM Comput Surv, 25(1), 375–414.

۱۰. Bedard, J. & Graham, L. & Jackson, C. (2008). “Archival evidence on detection and severity classification of Sarbanes-Oxley Section.” 404 internal control deficiencies Working.

۱۱. Chen, Z. & Yoon, J. (2010). IT auditing to assure a secure cloud computing. 6th World Congress on Services, 253–259.

۱۲. Da Veiga, A. & Eloff, J. (2007). “An information security governance framework”. Inf Syst Manag, 24(4), 361–372.

۱۳. Dhillon, G., & Torkzadeh, G. (2006). “Value-focused assessment of information system security in organizations”. Inf Syst J, 16(1), 293–314.

۱۴. Herath, T. & Rao, H. (2009). “Encouraging information security behaviors in organizations: role of penalties, pressures, and perceived effectiveness”. Decis Support Syst, 47(2), 154-165.

۱۵. Otero, A. R. (2015). “An information security control assessment methodology for organizations' financial information”. International Journal of Accounting Information Systems, 18: 26–45.

۱۶. shafeghati, S. & pilevari, N. (2013). “Provide a model for identifying and ranking the managerial factors affecting information security in organization by using vikor method; Case Study: Tehran University of Medical Sciences”. International Journal of Information, Security and System Management, 2(2), 183-189.

۱۷. Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC17799. Inf Manag J, 60–66.

۱۸. Singh, A. & Picot, A. & Kranz, J. & Gupta, M. O. (2013). “Information security management (ISM) practices: lessons from select cases from India and Germany”, Glob J Flex Syst Manag, 14(4), 239-255.

۱۹. van der Haar, H. & von Solms, R. (2003). “A model for deriving information security controls attribute profiles”, J Comput Secur, 22(3), 233–244.

۲۰. Yang , Y.-P. O. & Shieh, H.-M. & Tzeng, G.-H. (2013). “A VIKOR technique based on DEMATEL and ANP for information security risk control assessment”. Information Sciences, 232: 482–500.