# ارائه مدل سنجه گذاری عددی سیستم مدیریت امنیت اطلاعات (ISMS)

**اسماعیل رضایی [۱]، سجاد رمضانی [۲]، ابوالقاسم حسن پور [۳].**

**۱ - استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی کامپیوتر و صنایع، دانشگاه صنعتی بیرجند.**

**rezaei@birjandut.ac.ir**

**۲- دانشجوی دوره کارشناسی مهندسی کامپیوتر، دانشکده مهندسی کامپیوتر و صنایع، دانشگاه صنعتی بیرجند.**

**Sajjadramezaniii1378@gmail.com**

**۳- مدرس، گروه مهندسی کامپیوتر، دانشکده مهندسی کامپیوتر و صنایع، دانشگاه صنعتی بیرجند.**

**hassanpour@birjandut.ac.ir**

## چکیده

امروزه امنیت اطلاعات یکی از چالش‌های اصلی در عصر دانایی و اطلاعات محسوب می شود و حفاظت از اطلاعات در برابر دسترسی غیرمجاز ،تغییرات خرابکاری و افشا امری ضروری و اجتناب‌ناپذیر به شمار می‌رود؛ هدف این مقاله ارائه یک مدل ارزیابی عددی سیستم مدیریت امنیت اطلاعات (ISMS) از طریق ارزیابی اهمیت دسته‌بندی و کنترل موجود در ISMS است مدل ارزیابی عددی سیستم مدیریت امنیت اطلاعات که در این مقاله معرفی می شود، به‌منظور پایش و ارزیابی اجرای امنیت اطلاعات در سازمان‌ها و ارائه راهکارهای بهبود امنیت اطلاعات طراحی‌شده است. به‌منظور جمع آوری داده ها از روش کتابخانه ای مطالعات میدانی، پرسشنامه و مصاحبه استفاده شده است و مقالات، اسناد، دستورالعمل‌ها و مبانی مربوط به شناسایی چالش‌های امنیت اطلاعات بر اساس الزامات استاندارد ISO 27001 و ISO 27002 در این مجموعه موردبررسی قرارگرفته است.در جهت مشکلات و کاستی‌های امنیتی سازمان‌ها مدل‌های متنوعی ارائه‌شده است؛ مدل ارزیابی پیشنهادی در این مقاله با تمرکز بر سنجش درجه اهمیت دسته‌بندی

ها و کنترل‌های امنیتی، به سازمان‌ها کمک می‌کند تا کنترل‌های موجود در سیستم مدیریت امنیت اطلاعات را بهبود داده و سطوح امنیت اطلاعات خود را در برابر ضعف‌های امنیتی ارتقا دهند. با توجه به اینکه در هر سازمان نیازها و اولویت‌های مربوط به امنیت اطلاعات ممکن است متفاوت باشند، لذا بر این اساس در نظر داریم اهمیت هر یک از این دسته‌بندی‌ها و کنترل‌های موجود را مورد ارزیابی قرار داده و نمره اجرای سیستم مدیریت امنیت اطلاعات را در سازمان ها محاسبه کرده و در نهایت یک چهارچوب برای اولویت‌بندی کنترل‌ها در سازمان‌ها فراهم می‌سازد.

**کلمات کلیدی:** امنیت سایبری، سیستم مدیریت امنیت اطلاعات (ISMS)، استاندارد ISO/IEC 27001، سنجه گذاری عددی.

## ۱. مقدمه

فناوری اطلاعات بر زندگی انسان و حیات سازمان‌ها تأثیرات بسزایی دارد. امروزه امنیت اطلاعات، بزرگ‌ترین چالش در عصر فناوری اطلاعات محسوب می‌شود و حفاظت از اطلاعات در مقابل دسترسی‌های غیرمجاز،تغییرات،خرابکاری‌ها و افشا، امری ضروری و اجتناب‌ناپذیر به شمار می‌رود. ازاین‌رو امنیت دارایی‌های اطلاعاتی، برای تمامی سازمان‌ها امری حیاتی بوده و مستلزم یک مدیریت اثربخش است[2][1].

### ۱-۱ سیستم مدیریت امنیت اطلاعات (ISMS)

سیستم مدیریت امنیت اطلاعات یا ISMS (Information Security Management System) یک چهارچوب استاندارد برای شناسایی، مدیریت و به حداقل رساندن احتمال وقوع مخاطراتی که سازمان‌ها به‌واسطه از دست دادن اطلاعات خود با آن‌ها مواجه می‌شوند؛ تهدیداتی که مشتمل بر : تهدیدات داخلی سازمان، تهدیدات خارجی سازمان، تهدیدات اتفاقی، تهدیدات ناشی از خطاهای عمدی و غیرعمدی است. امروزه سازمان‌ها بسیاری از فرصت‌های تجاری خود را به لحاظ از دست دادن اطلاعات ارزشمند خود از دست می‌دهند. هدف اصلی ISMS برقراری مکانیسمی در جهت حفاظت از این فرصت‌ها است. سیستم مدیریت امنیت اطلاعات بر پایه استاندارد بین‌المللی ISO/IEC 27001 و ISO/IEC 27002 ساخته‌شده است.

### ۲-۱- دسته‌بندی‌های سیستم مدیریت امنیت اطلاعات (ISMS)

این استاندارد شامل چهار دسته کنترل کلیدی است که شامل کنترل‌های سازمانی، کنترل‌های فیزیکی، کنترل‌های فناوری و کنترل‌های نیروی انسانی می‌باشد. این دسته‌بندی‌ها به‌طورکلی شامل ۹۳ کنترل که همه آن‌ها به‌طور جامع برای ایجاد و حفظ امنیت اطلاعات در سازمان‌ها ضروری هستند[2] [3] [4].

کنترل‌های سازمانی شامل سیاست‌ها، رویه‌ها و فرآیندهای مدیریتی است که سازمان برای حفظ امنیت اطلاعات خود اتخاذ می‌کند. این شامل مواردی مانند تعیین نقش‌ها و مسئولیت‌ها، آموزش و آگاهی کارکنان، مدیریت ریسک و رخدادهای امنیتی و برنامه‌ریزی برای حفظ پیوستگی عملیات سازمان است[3][4].

کنترل‌های فیزیکی شامل اقداماتی است که به‌منظور حفاظت از محیط فیزیکی و منابع سازمان اتخاذ می‌شود. این شامل مواردی مانند کنترل دسترسی فیزیکی، محدودیت دسترسی به تجهیزات حساس، مانیتورینگ و کنترل محیط فیزیکی سازمان و مدیریت دسترسی به تسهیلات فیزیکی است.

کنترل‌های فناوری شامل اقداماتی است که برای محافظت و مدیریت منابع فناوری اطلاعات اتخاذ می‌شود. این شامل مواردی مانند مدیریت دسترسی لازم برای سیستم‌ها و شبکه‌ها، مانیتورینگ و لاگ‌گیری، حفاظت از داده‌ها و رمزنگاری، مدیریت آسیب‌پذیری‌ها و برنامه‌های کاربردی و مدیریت امنیت شبکه‌ها و تجهیزات فنی دیگر است[3][4].

کنترل‌های نیروی انسانی شامل سیاست‌ها و رویه‌هایی است که برای مدیریت امنیت اطلاعات در ارتباط با کارکنان سازمان به کار گرفته می‌شود. این شامل مواردی مانند فرآیندهای استخدام و تربیت کارکنان، آگاهی و آموزش امنیت اطلاعات، مدیریت دسترسی کارکنان به اطلاعات حساس و برنامه‌ریزی برای مدیریت واکنش به رفتارهای نامطلوب کارکنان است[3][4].

با ترکیب این چهار حوزه کنترلی، سازمان‌ها قادر خواهند بود تا یک سیستم مدیریت امنیت اطلاعات جامع را پیاده‌سازی کنند و از تهدیدات امنیتی محافظت کنند. در این مقاله، به بررسی این چهار حوزه کنترلی و کنترل‌های موجود در ISMS با تأکید بر استاندارد ISO/IEC 27001 و ISO/IEC 27002 خواهیم پرداخت. تحلیل و بررسی این کنترل‌ها به سازمان‌ها کمک می‌کند تا نیازهای امنیتی خود را شناسایی کرده و راهکارهای مناسبی را برای حفظ امنیت اطلاعات خود اتخاذ کنند[4][3].

اما در این مقاله، تمرکز ما بر روی تفاوت درجه اهمیت دسته‌بندی‌ها و کنترل‌های موجود در ISMS در جهت ارزیابی پیاده‌سازی کنترل‌های امنیتی در یک سازمان است. سنجه گذاری دسته‌بندی کنترل‌ها به‌عنوان یک روش برای سازمان‌دهی

کنترل‌های امنیتی، بسیار حائز اهمیت است زیرا به کمک آن سازمان قادر خواهد بود تا بر روی نقاط ضعف و نیازهای امنیتی مهم متمرکز شود.

در این مقاله، یک مدل پیشنهادی ارزیابی عددی برای سیستم مدیریت امنیت اطلاعات ارائه‌شده است. با استفاده از این مدل، سازمان می‌تواند بهبودهای لازم را در امنیت اطلاعات خود اعمال کند و برنامه‌هایی را برای مدیریت ریسک‌های امنیتی تعیین کند.

## ۲- روش پیشنهادی

### ۲-۱ مدل ارزیابی سیستم مدیریت امنیت اطلاعات

این مدل ارزیابی دارای سه فاز بوده است:

فاز اول شامل شناسایی دسته‌بندی‌ها و کنترل‌های امنیتی موجود در سیستم مدیریت امنیت اطلاعات است. در این فاز، پس از استخراج این کنترل‌ها از ISMS پرسشنامه‌ای بر مبنای طیف لیکرت طرح شد و شامل سؤالاتی در رابطه با اولویت‌بندی و درجه اهمیت هر دسته و کنترل‌ها است[6][5].

فاز دوم مدل ارزیابی شامل تخصیص وزن به هر کنترل امنیتی بر اساس درجه اهمیت آن است. با استفاده از اطلاعات جمع‌آوری‌شده در فاز اول، وزنی به هر کنترل امنیتی اختصاص داده می‌شود که نشان‌دهنده درجه اهمیت آن کنترل در سازمان است. این وزن بر اساس ارزشیابی‌های کمی و کیفی صورت می‌گیرد و به سازمان کمک می‌کند تا کنترل‌هایی که نیاز به بهبود دارند را شناسایی کند.

فاز سوم مدل ارزیابی شامل تحلیل و ارزیابی نتایج است. در این فاز، امتیازهای دریافتی برای هر کنترل امنیتی موردبررسی قرار می‌گیرد و نتایج نشان می‌دهند که آیا کنترل‌های موجود در سازمان به‌درستی پیاده‌سازی شده‌اند و سطوح امنیت اطلاعات مناسب را فراهم می‌کنند یا خیر.

در عمل، ارزیابی و مدیریت امنیت اطلاعات به یک‌روند پیچیده و چندجانبه نیاز دارد و این روش تنها یکی از ابزارهای موجود است که می‌تواند در این فرآیند مفید باشد.

با توجه به تفاوت اهمیت دسته‌بندی کنترل‌ها، که در نظر داریم این موضوع را در ارزیابی پیاده‌سازی کنترل‌های امنیتی در یک سازمان دخیل کنیم.

کنترل‌های سازمانی و غیره که در دسته‌بندی‌های ISMS در چهار دسته قرار می‌گرفت از یک درجه اهمیت برخوردار نیستند، در اینجا سؤالی مطرح می‌گردد برای ارزیابی درجه اهمیت این دسته‌بندی‌ها و کنترل‌ها چه کنیم؟

برای این منظور پرسشنامه‌ای در خصوص درجه اهمیت این دسته‌بندی‌ها و کنترل‌های موجود در استاندارد ISMS طراحی‌شده است و در اختیار خبرگان امنیت سایبری قرار گرفت[5][7].

در این پرسشنامه نظر هر یک از متخصصین درباره درجه اهمیت هر یک از دسته‌ها و کنترل‌ها جمع‌آوری می‌شود و بر اساس تحلیل هریک از نظرات وزنی به هر یک از دسته‌ها و کنترل‌ها اختصاص می‌گردد؛ به‌نوعی پس از تکمیل پرسشنامه و دریافت نظرات متخصصین حوزه امنیت سایبری یک خروجی دریافت خواهیم کرد.

محاسبات این مدل با میانگین‌گیری وزنی این نظرات که می‌توان از نرم‌افزارهای آماری مانند SPSS نیز استفاده نمود، محاسبه خواهد شد.

این خروجی اهمیت هر دسته یا هر مورد کنترل را به‌صورت یک مقدار کمی نشان می‌دهد به‌نوعی وزن هر دسته را مشخص می‌کند.

### ۲-۲- طراحی پرسشنامه‌ها

هدف از طراحی پرسشنامه‌ها ارزیابی درجه اهمیت دسته‌ها و کنترل‌ها است. در هر یک از موارد از طیف لیکرت شامل ۵ سطح اهمیت (خیلی کم، کم، متوسط، زیاد، خیلی زیاد) استفاده‌شده است. در راستای این موضوع ۵ پرسشنامه طراحی‌شده است[7][5].

- پرسشنامه سنجه گذاری درجه اهمیت دسته‌بندی‌های ISMS
  - در این پرسشنامه ۴ دسته کنترل ارزیابی اهمیت می‌شوند.
- ۴ پرسشنامه سنجه گذاری درجه اهمیت کنترل‌های موجود در هر دسته‌بندی ISMS
  - در این پرسشنامه‌ها به‌طورکلی ۹۳ مورد کنترل، ارزیابی اهمیت می‌شوند.

### ۲-۳- سنجه گذاری عددی

سنجه گذاری عددی ارزیابی دسته‌بندی‌ها و کنترل‌ها در این روش پیشنهادی، لازم است درجه اهمیت انجام این کنترل‌ها در سازمان را که به‌صورت کیفی ثبت می‌شود به‌صورت کمی ثبت کنیم.

در این روش سنجه گذاری عددی سیستم مدیریت امنیت اطلاعات ارزیابی انجام‌شده در قالب پنج مقدار «خیلی کم»، «کم»، «متوسط»، «زیاد» و «خیلی زیاد» است در جهت سنجه گذاری عددی می‌توان به شرح زیر این مقادیر کیفی را به مقادیر کمی تبدیل کنیم.

- خیلی کم معادل امتیازی صفر
- کم معادل امتیازی ۰.۲۵
- متوسط معادل امتیازی ۰.۵۰
- زیاد معادل امتیازی ۰.۷۵
- خیلی زیاد معادل امتیازی ۱

### ۲-۴- مدل محاسباتی سنجه گذاری عددی (ISMS)

بیان مدل ریاضی برای محاسبه اهمیت کنترل‌های ISMS در این روش پیشنهادی تعریف پارامترها و فرمول نهایی محاسبه نمره اجرای سیستم مدیریت امنیت اطلاعات به‌صورت زیر می‌توان شرح داد:

- پارامترها
  - پارامترهای این مدل شامل مجموعه‌ای از ضرایبی است که از طریق تحلیل نظرات متخصصین امنیت به دست می‌آید.

**جدول ۱ – پارامترها در مدل سنجه گذاری عددی (ISMS)**

| پارامتر | تعریف | مقدار بازه |
|---|---|---|

| | | |
|---|---|---|
| $C_C$ | ضریب کنترل | [1,5] |
| $D_C$ | ضریب دسته | [1,5] |
| S | نمره | [0,1] |

- فرمول سنجه گذاری

مطابق با پارامترها فرمول نهایی که می‌توان برای این مدل ارائه کرد به شرح زیر است:

$$Q = \sum_{c=1}^{c} S \times C_c \times D_c \qquad (1)$$

با توجه به فرمول ارائه‌شده و بازه‌های تعیین‌شده برای هر پارامتر مقادیر مینیمم و ماکزیمم اهمیت برای پیاده‌سازی آن کنترل‌ها به‌صورت زیر خواهد بود:

مینیمم مقدار برای هر کنترل برابر صفر است.

ماکزیمم مقدار برای کنترل‌ها با درجه اهمیت خیلی زیاد برابر ۲۵ خواهد بود.

**تذکر:** مقدار S نمره اجرای کنترل‌های سیستم مدیریت اطلاعات است که توسط ارزیاب به سازمان داده خواهد شد.

## ۵-۲- تحلیل داده‌ها و استخراج ضرایب کنترل‌ها و دسته‌های ISMS

از مهم‌ترین مراحل هر پژوهش تجزیه‌وتحلیل داده‌های جمع‌آوری‌شده با استفاده از ابزارهای معتبر است. پس از جمع‌آوری داده‌ها مرحله جدیدی از فرایند که مرحله‌ی تجزیه‌وتحلیل داده‌ها است، شروع می‌شود.

در این مرحله با استفاده از روش قیدشده در مقاله و با تکیه‌بر معیار عقل، سعی می‌شود که داده‌ها را در جهت پاسخ سؤالات این پژوهش و ارزیابی آن‌ها موردبررسی قرار داده شود. به‌منظور انجام صحیح این امر، داده‌های جمع‌آوری‌شده بایستی به‌طور علمی و با روش‌های آماری مناسب، مورد پردازش قرارگرفته و به‌صورت اطلاعات قابل‌استفاده برای تصمیم‌گیری و مراحل بعدی تبدیل شود[8] [9].

به‌طورکلی، پس از تکمیل پرسشنامه و گردآوری داده‌ها، نوبت به استخراج، طبقه‌بندی داده‌ها و تحلیل دانش نهفته در آن‌ها می‌رسد که با تهیه جداول توزیع فراوانی آغاز می‌شود.

با توجه به پرسشنامه‌ها و داده‌های جمع‌آوری‌شده از نظرات خبرگان امنیت سایبری با استفاده از نرم‌افزار آماری SPSS فراوانی نظرات میانگین وزنی هر دسته کنترلی و هر مورد از کنترل‌ها محاسبه خواهد شد و در این بخش مورد تحلیل و بررسی قرار می‌گیرد.

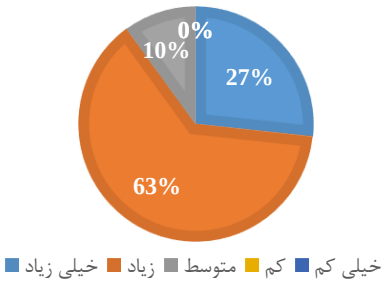
### ۱-۵-۲- تحلیل داده‌های مربوط به دسته‌بندی کنترل‌ها

مطابق با سؤالات طرح‌شده به تعداد ۹۷ سؤال از ۴ دسته کنترل موجود و داده‌های جمع‌آوری‌شده از جامعه هدف ۳۰ عضوی از میان خبرگان امنیت و با توجه به فراوانی داده‌ها و میانگین وزنی داده‌ها، اهمیت دسته‌بندی کنترل‌های سیستم مدیریت امنیت اطلاعات در جداول زیر قیدشده است[8][9].

**جدول ۲- توزیع فراوانی گروه نمونه کنترل‌های سازمانی**

| کنترل های سازمانی | فراوانی | درصد |
|---|---|---|

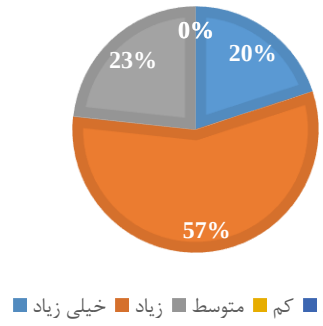
| | | |
|---|---|---|
| خیلی زیاد | 8 | 26.7 |
| زیاد | 19 | 63.3 |
| متوسط | 3 | 10 |
| کم | 0 | 0 |
| خیلی کم | 0 | 0 |
| مجموع | 30 | 100 |




**نمودار ۱- توزیع فراوانی گروه نمونه کنترل‌های سازمانی**

**جدول ۳- توزیع فراوانی گروه نمونه کنترل‌های نیروی انسانی**

| کنترل‌های نیروی انسانی | فراوانی | درصد |
|---|---|---|
| خیلی زیاد | 6 | 20 |
| زیاد | 17 | 56.7 |
| متوسط | 7 | 23.3 |
| کم | 0 | 0 |
| خیلی کم | 0 | 0 |
| مجموع | 30 | 100 |

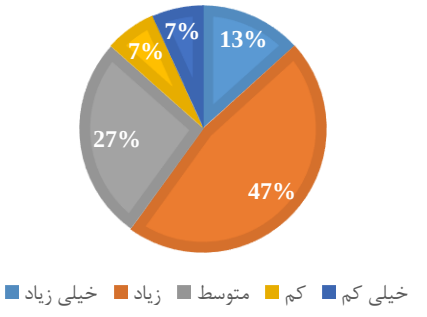



**نمودار ۲- توزیع فراوانی گروه نمونه کنترل‌های نیروی انسانی**

**جدول ۴- توزیع فراوانی گروه نمونه کنترل‌های فیزیکی**

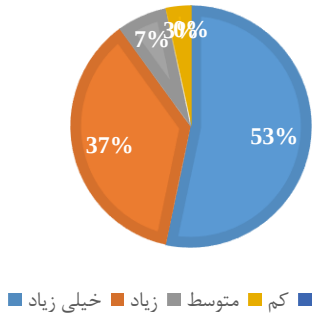
| کنترل‌های فیزیکی | فراوانی | درصد |
|---|---|---|
| خیلی زیاد | 4 | 13.3 |
| زیاد | 14 | 46.7 |
| متوسط | 8 | 26.7 |
| کم | 2 | 6.7 |
| خیلی کم | 2 | 6.7 |
| مجموع | 30 | 100 |

**نمودار ۳- توزیع فراوانی گروه نمونه کنترل‌های فیزیکی**




**جدول ۵- توزیع فراوانی گروه نمونه کنترل‌های فناوری**

| کنترل‌های فناوری | فراوانی | درصد |
|---|---|---|
| خیلی زیاد | 16 | 53.3 |
| زیاد | 11 | 36.7 |
| متوسط | 2 | 6.7 |
| کم | 1 | 3.3 |
| خیلی کم | 0 | 0 |
| مجموع | 30 | 100 |




**نمودار ۴- توزیع فراوانی گروه نمونه کنترل‌های فناوری**

**تذکر:** در تحلیل و بررسی تمامی نمودارهای این پژوهش با توجه به تعداد بالای موارد کنترلی در هر دسته و محدودیت در بیان آن‌ها در این مقاله برای درک بهتر سند ISMS ISO 27001 و ISMS ISO 27002را نیز بررسی نمایید.

### ۲-۲-۵- ضریب دسته‌بندی کنترل‌ها ($D_c$)

با توجه به جداول ۱ تا ۴ که به تحلیل فراوانی داده‌های هر دسته پرداخته شد و میانگین وزنی داده‌ها ضریب دسته‌بندی کنترل‌ها در این مدل پیشنهادی محاسبه می‌شود.

ضرایب به‌دست‌آمده به شرح زیر است:

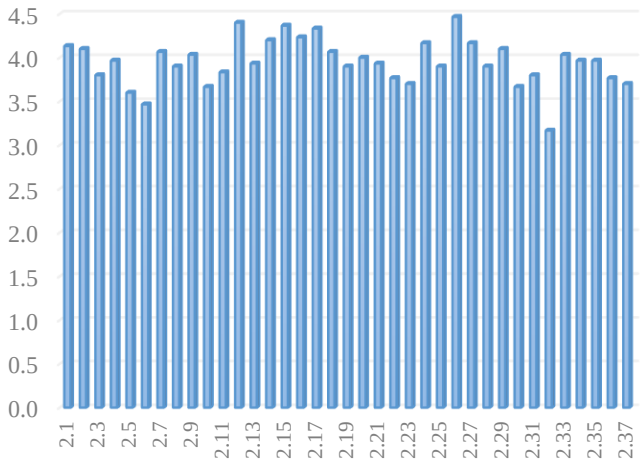
- ضریب دسته‌بندی کنترل‌های سازمانی معادل ۴.۲
- ضریب دسته‌بندی کنترل‌های نیروی انسانی معادل ۴
- ضریب دسته‌بندی کنترل‌های فیزیکی معادل ۳.۵
- ضریب دسته‌بندی کنترل‌های فناوری معادل ۴.۴

**تذکر**: ضریب دسته‌بندی کنترل‌ها در کل فرآیند مدل محاسباتی سنجه گذاری عددی آن دسته ثابت خواهد بود.

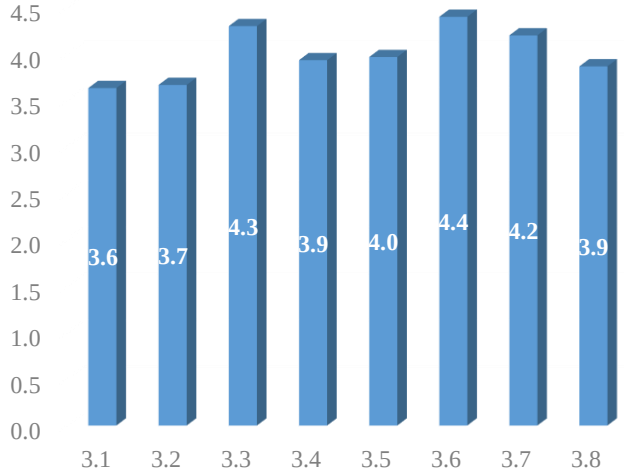
### ۳-۲-۵- بررسی ضریب اهمیت هر مورد از کنترل‌ها در هر دسته‌بندی ($C_c$)

محاسبه ضریب هر مورد از کنترل‌ها مطابق با فراوانی داده‌ها از ارزیابی انجام‌شده جامعه هدف ۳۰ عضوی و با استفاده از میانگین وزنی تعیین می‌گردد.

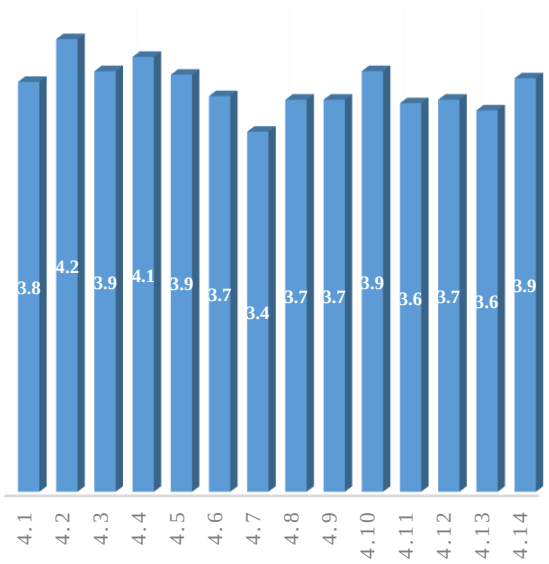
ضریب اهمیت هر یک از موارد کنترل‌ها پس از محاسبه در قالب نمودارها، به شرح زیر است:



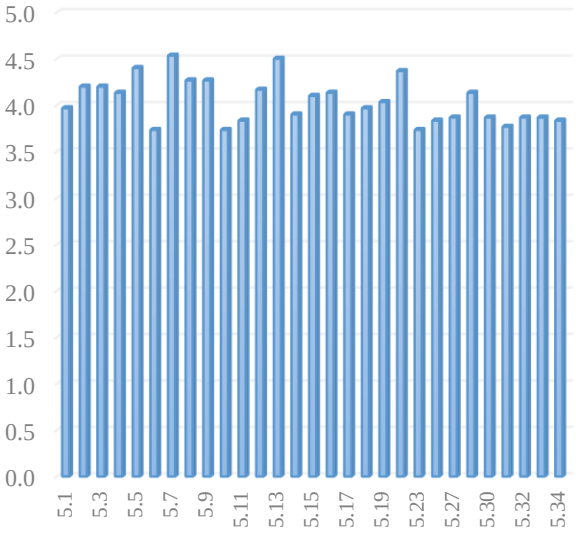

**نمودار ۵- ضریب اهمیت هر مورد از کنترل‌های سازمانی**




**نمودار ۶- ضریب اهمیت هر مورد از کنترل‌های نیروی انسانی**




**نمودار ۷- ضریب اهمیت هر مورد از کنترل‌های فیزیکی**




**نمودار ۸- ضریب اهمیت هر مورد از کنترل‌های فناوری**

### ۳. از مزایای استفاده از مدل سنجه گذاری عددی

- ارزیابی سیستماتیک: مدل ارزیابی عددی ارائه‌شده، رویکردی سیستماتیک و منظم برای ارزیابی امنیت اطلاعات در سازمان‌ها فراهم می‌کند. این مدل با استفاده از روش‌های مشخص و پارامترهای قابل‌اندازه‌گیری، امکان ارزیابی دقیق و قابل تکرار را فراهم می‌کند.
- تطبیق با نیازهای سازمان: مدل قابلیت سفارشی‌سازی و تطبیق با نیازهای خاص هر سازمان را دارا است. این امر به سازمان‌ها امکان می‌دهد تا مدل را بر اساس ساختار، اندازه و خصوصیات خودتنظیم کنند و نتایج متناسب با شرایط خود را دریافت کنند.
- بهبود امنیت اطلاعات: این مدل با تحلیل و ارزیابی کنترل‌های موجود، به بهبود وضعیت امنیت داده‌های سازمان کمک می‌کند.

### ۴. نتیجه‌گیری

یکی از مهم‌ترین چالش‌ها و دغدغه‌ها در سیستم مدیریت امنیت اطلاعات، پیاده‌سازی و عملیاتی شدن واقعی این سیستم و تداوم مؤثر آن در سازمان است. هدف این مقاله ارائه یک مدل سنجه گذاری عددی سیستم مدیریت امنیت اطلاعات بر اساس استاندارد ISO / IEC 27001 است. این تحقیق انجام‌شده می‌تواند یک مبنایی در جهت پیاده‌سازی ISMS در یک سازمان باشد.

در این مقاله، ما به بررسی مدل ارزیابی امنیت اطلاعات پرداختیم و نتایج به‌دست‌آمده را بررسی کردیم.
از طریق ارزیابی امنیت اطلاعات، سازمان‌ها قادر خواهند بود تا ضعف‌ها و آسیب‌پذیری‌های موجود در سیستم‌ها و شبکه‌های خود را شناسایی کنند. در این مقاله، مدل سنجه گذاری امنیت اطلاعات را از جنبه درجه اهمیت کنترل‌ها و دسته‌بندی‌های ISMS موردبررسی قرار گرفت.

بر اساس پایش به‌عمل‌آمده استفاده از مدل سنجه گذاری امنیت اطلاعات می‌تواند بهبود قابل‌توجهی در سطح امنیتی سازمان‌ها و شرکت‌ها به همراه داشته باشد. با استفاده از این مدل، سازمان‌ها قادر خواهند بود تا به‌طور مداوم عملکرد امنیتی خود را ارزیابی کنند و نقاط ضعف را شناسایی کرده و تصمیماتی جهت بهبود آن‌ها بگیرند. علاوه بر این، استفاده از مدل ارزیابی امنیت اطلاعات به سازمان‌ها کمک می‌کند تا با رعایت استانداردها و راهنماهای امنیتی، از تهدیدات امنیتی پیشگیری کنند و در صورت وقوع حملات، آمادگی لازم برای مقابله با آن‌ها را داشته باشند.

از یافته‌های این پژوهش می‌توان نتیجه گرفت که بر اساس نظر جامعه آماری ما در این مدل پیشنهادی (سنجه گذاری عددی) به ترتیب، کنترل‌های فناوری، کنترل‌های سازمانی، کنترل‌های نیروی انسانی و کنترل‌های فیزیکی اهمیت دارند.

با توجه به نتایج به‌دست‌آمده از ارزیابی انجام‌شده و فرمول ارائه‌شده و بازه‌های تعیین‌شده برای هر پارامتر مقادیر مینیمم و ماکزیمم اهمیت برای پیاده‌سازی آن کنترل‌ها به‌صورت زیر خواهد بود:
مینیمم مقدار برای هر کنترل برابر صفر است.

ماکزیمم مقدار در محاسبه نمره اجرای کنترل‌های سیستم مدیریت امنیت اطلاعات در هر دسته به شرح زیر خواهد بود :

- ماکزیمم نمره کنترل‌های سازمانی معادل ۶۱۴
- ماکزیمم نمره کنترل‌های نیروی انسانی معادل ۱۲۸
- ماکزیمم نمره کنترل‌های فیزیکی معادل ۱۸۵.۶
- ماکزیمم نمره کنترل‌های فناوری معادل ۵۱۵.۲

## ۵. مراجع

[1] فاطمه و ر. رضا, "ارائه مدلی برای پایش بلوغ امنیت اطلاعات," ج ۱۶, ش ۶۴۰۰۱۳۲۵, صص ۴۱–۵۱, ژانویه ۲۰۲۰.

[2] سیدحامد هنرپرورتمیز، سعید رضایی،حامد حسین نسب, *نظام مدیریت امنیت اطلاعات*, ج ۱. تهران: انتشارات ماهواره, ۱۳۹۸.

[3] "SecManagmentSystemsReq.pdf." [آنلاین]. قابل دسترس در: دسترسی: ۱۳ می ۲۰۲۳. https://eldritchdata.neocities.org/PDF/CS/SecManagmentSystemsReq.pdf

[4] S. N. V. Schweizerische, "Information technology-Security techniques-Information security management systems-Requirements," *ISOIEC Int. Stand. Organ.*, 2013.

[5] "تحقیق در مورد طراحی پرسشنامه: خلاصه ای از ادبیات - پترا لیتز، ۲۰۱۰." دسترسی: ۱۴ آگوست ۲۰۲۳. [آنلاین]. قابل دسترس در : https://journals.sagepub.com/doi/10.2501/S147078530920120X

[6] J. A. Krosnick, "Questionnaire Design," در *The Palgrave Handbook of Survey Research*, D. L. Vannette و J. A. Krosnick, ویراستاران, Cham: Springer International Publishing, 2018, صص ۴۳۹–۴۵۵. doi: 10.1007/978-3-319-54395-6_53.

[7] A. Asosheh, B. Dehmoubed, و A. Khani, "A new quantitative approach for information security risk assessment," در *2009 2nd IEEE International Conference on Computer Science and Information Technology*, آگوست ۲۰۰۹, صص ۲۲۲–۲۲۷. doi: 10.1109/ICCSIT.2009.5234391.

[8] مهدی اکرامی بیرجند نژاد- دکتر حسین حکیم پور, "بررسی تأثیر تجارت الکترونیک در توسعه صادرات شرکت های کوچک و متوسط," دانشگاه آزاد اسلامی, بیرجند, ۱۳۹۹.

[9] سهیلا یزدی زاده-دکتراسماعیل رضایی, "تحلیل راهبردی استفاده از بیت کوین در اقتصاد ایران," پایان نامه درجه کارشناسی ارشد, دانشگاه آزاد اسلامی, بیرجند, ۱۴۰۱.