ارائه مدلی برای پایش بلوغ امنیت اطلاعات

فاطمه اخوان*
دانشگاه آزاد اسلامی، تهران، ایران
f63akhavan@gmail.com

رضا رادفر**
دانشگاه علوم تحقیقات، تهران، ایران
radfar@gmail.com

تاریخ دریافت: ۱۳۹۸/۰۱/۲۸
تاریخ اصلاحات: ۱۳۹۹/۰۴/۰۱
تاریخ پذیرش: ۱۳۹۹/۰۴/۲۸

چکیده

امروزه امنیت اطلاعات یکی از چالش‌های اصلی در عصر دانایی و اطلاعات محسوب می‌شود و حفاظت از اطلاعات در برابر دسترسی غیرمجاز، تغییرات، خرابکاری و افشا، امری ضروری و اجتناب‌ناپذیر به شمار می‌رود. هدف و انگیزه این مقاله به دلیل ارائه مدل بلوغ امنیت اطلاعات برای پایش اجرای امنیت در سازمان‌ها و ارائه بهترین شیوه‌های پیاده‌سازی امنیت است. پژوهش حاضر که در یکی از شرکت‌های زیرمجموعه صنعت نفت انجام شده است، به صورت روش آمیخته کیفی ـ کمی انجام شده است. به منظور جمع‌آوری داده‌ها از روش کتابخانه‌ای، مطالعات میدانی، پرسشنامه و مصاحبه استفاده شده است و مقالات، اسناد، دستورالعمل‌ها و مبانی مربوط به شناسایی چالش‌های امنیت فناوری اطلاعات براساس الزامات استاندارد ISO 27001 در این مجموعه ستادی مورد بررسی قرار گرفته است. برای شناسایی موانع و کاستی‌های امنیتی یک سازمان خاص، مدل‌های مختلفی ارائه شده است. هدف، شناسایی یک فاصله بین تئوری و عمل می‌باشد که می‌تواند از طریق رویکرد فرایند محور به هم نزدیک شوند. مدل بلوغی که در این پروژهش معرفی و مورد استفاده قرار می‌گیرد، یک نقطه شروع برای پیاده‌سازی امنیت، یک دیدگاه عمومی از امنیت و یک چارچوب برای اولویت‌بندی عملیات، فراهم می‌سازد. این مدل بلوغ امنیت اطلاعات دارای ۵ فاز می‌باشد. مدل بلوغ امنیت اطلاعات به‌عنوان ابزاری جهت ارزیابی توانایی سازمان‌ها برای مطابقت با اهداف امنیت، یعنی، محرمانگی، یکپارچگی و در دسترس‌بودن و جلوگیری از حملات و دستیابی به مأموریت سازمان علی‌رغم حملات و حادثه‌ها می‌باشد. نتایج ارزیابی نشان می‌دهد که سازمان‌هایی که سرمایه‌گذاری‌های امنیتی را در پیش رو دارند، باید ضرورت به‌کارگیری امنیت اطلاعات در سازمان توسط مدیران عالی درک شده باشد، و علاوه بر اقداماتی که در زمینه امنیت محیط فیزیکی، شبکه و کامپیوترهای شخصی و کنترل‌های دسترسی و رمزنگاری صورت گرفته است آموزش و فرهنگ‌سازی لازم پیاده‌سازی شود.

واژگان کلیدی

امنیت اطلاعات؛ سیستم مدیریت امنیت اطلاعات (ISMS)؛ مدل بلوغ؛ مدل بلوغ امنیت اطلاعات؛ استاندارد ISO27001.

۱- مقدمه

فناوری اطلاعات به‌طور قابل توجهی بر زندگی انسان تأثیر می‌گذارد. با این حال، امنیت اطلاعات هنوز هم یک نگرانی مهم برای کاربران و سازمان‌ها است. فناوری تنها نمی‌تواند یک محیط امن برای اطلاعات را تضمین کند؛ جنبه‌های انسانی امنیت اطلاعات، علاوه بر جنبه‌های فناورانه، باید مورد توجه قرار گیرد. کمبود آگاهی امنیتی، نادیده گرفتن، سهل‌انگاری، بی‌تفاوتی و مقاومت، ریشه اشتباهات کاربران است. اما امنیت اطلاعات هنوز نگرانی بحث‌انگیز است. ابزارهای امنیتی سخت‌افزاری و نرم‌افزاری (مانند آنتی ویروس، آنتی‌اسپم، آنتی فیشینگ، فایروال، احراز هویت و سیستم‌های تشخیص نفوذ) جنبه‌های فناورانه هستند که امنیت اطلاعات را بر عهده دارند، اما آنها نمی‌توانند یک محیط امن را برای اطلاعات تضمین کنند. در حال حاضر هکرها به جای استفاده از نقص‌های سیستم‌های رایانه‌ای، نقص‌ها و ضعف‌های انسان‌ها را هدف قرار می‌دهند؛ (مثال‌هایی از اشتباهات کاربر عبارتند از رفتار امنیتی نامناسب، نام کاربری و گذرواژه نامناسب، نوشتن گذرواژه بر روی کاغذ در دسترس، به اشتراک‌گذاری نام کاربری و گذرواژه با همکاران، بازکردن ایمیل‌های ناشناخته و دانلود فایل پیوست این ایمیل‌ها، و همچنین دانلود نرم‌افزار از اینترنت.) رفتارهای قابل قبول اطلاعات باید به‌طور ایده‌آل با جنبه‌های تکنیکی ترکیب شوند. بنابراین، در محیط امنیتی اطلاعات، استفاده از روش‌های مختلف امنیتی برای کاهش خطر نقض امنیت اطلاعات ضروری است. وب جهان‌گستر محیطی عظیم و پویا است که در آن هکرها از روش‌های جدید و متفاوت برای رسیدن به اهدافشان و نقص امنیت استفاده می‌کنند [۳]. با توجه به وابستگی سازمان‌ها به اطلاعات و سیستم‌های مربوط به آن و ظهور عصر دانایی و اطلاعات در قرن حاضر، با

* نویسنده مسئول- دانشجوی دکترای مدیریت فناوری اطلاعات- مدیریت خدمات و توسعه فناوری، دانشگاه آزاداسلامی واحد تهران مرکزی
** عضو هیأت‌علمی و مدیرگروه مدیریت تکنولوژی و مدیریت صنعتی دانشگاه آزاد اسلامی واحد علوم و تحقیقات

تهدیدهای مربوط به اطلاعات و سیستم نیز مواجه هستند که روز به روز پیچیده‌تر می‌شود. خطرات مربوط به امنیت اطلاعات، چالش بزرگی برای بسیاری از سازمان‌ها است. این خطرات ممکن است عواقب وخیمی از جمله، از دست‌دادن شهرت سازمان و آسیب‌های مالی سنگین در پی داشته باشد. چشم‌پوشی از امنیت اطلاعات به منزله مواجه با انواع مشکلات و مسائل پرمخاطره است که ممکن است در انجام هر کاری با آن روبه‌رو شد. لذا امنیت اطلاعات برای سازمان، نیاز و یک ضرورت است. اما چگونه سازمان‌ها و شرکت‌ها اطمینان از سطح مقاومت کافی سیستم‌های امنیتی خود در برابر این تهدیدات و میزان سرمایه‌گذاری‌هایی مؤثر داشته باشند؟ با توجه به این‌که هیچ فرمولی نمی‌تواند امنیت را به‌طور کامل تضمین کند، به هرحال به یک سری معیارها و استانداردها برای دستیابی به سطح مناسبی از امنیت اطلاعات نیاز داریم تا منابع سازمان به‌طور مؤثر مورد استفاده قرار گرفته و بهترین شیوه امنیتی اتخاذ شود. در به‌کارگیری استانداردهای امنیت اطلاعات، ابتدا باید به مطابقت با استاندارد اصلی تأکید کنیم و توجه داشته باشیم که بومی‌سازی یا متناسب‌سازی آن‌ها ممکن است معضلاتی به وجود بیاورد.

رویکرد کسب وکار و چارچوب مدیریت مخاطرات سازمان از طریق ایجاد و نگهداشت سیستم (ISMS)[1] مدیریت امنیت اطلاعات، زمینه‌ای را برای شناسایی، ارزیابی، کنترل و مدیریت مخاطرات مرتبط با امنیت اطلاعات در سازمان و براساس معیارهای حفظ محرمانگی، صحت و در دسترس‌بودن دارایی‌های اطلاعاتی مهیا می‌نماید. هنگامی‌که سازمان نسبت به تعریف پروژه طراحی سیستم مدیریت امنیت اطلاعات اقدام می‌نماید و اهداف مشخصی را برای دستیابی به امنیت در سازمان تعیین می‌کند، باید شناخت کلانی نسبت به وضعیت خود و توانایی دستیابی به این اهداف داشته باشد. بنابراین لازم است سازمان با استفاده از ابزاری به پایش سطح بلوغ امنیتی جهت شناسایی و تحلیل کاستی‌ها و شکاف‌های موجود در سازمان در راه رسیدن به اهداف امنیتی و اطلاعات کلانی درخصوص وضعیت تجهیزات سخت‌افزاری و نرم‌افزاری مورد استفاده در سازمان، شبکه‌های ارتباطی و امنیت فیزیکی آن به‌دست آید. بسیاری از سازمان‌ها کارکنان خود را ضعیف‌ترین حلقه در امنیت اطلاعات در نظر می‌گیرند، اما همین کارکنان می‌توانند سرمایه‌های بزرگی در تلاش برای کاهش خطر امنیت سیستم‌های اطلاعاتی باشند.

۲- مروری بر ادبیات

امنیت اطلاعات شامل دسترسی، یکپارچگی و محرمانه‌بودن است. امنیت سایبری شامل ابعاد اضافی است که فراتر از مرزهای رسمی امنیت اطلاعات است، از جمله انسان‌ها در ظرفیت شخصی و جامعه به‌طور گسترده‌ای می‌تواند آسیب ببینند یا آسیب برسانند، لذا همکاری در سازمان‌ها برای ایجاد یک محیط امنیتی برای امنیت اطلاعات و امنیت سایبری ضروری است [۴]. رفتار امنیت اطلاعات مناسب، علاوه بر جنبه‌های فناورانه امنیت اطلاعات، ریسک نقض امنیت اطلاعات در سازمان را کاهش می‌دهد. مطالعات قبلی نشان داده است که آگاهی از امنیت اطلاعات کارکنان نقش مهمی در کاهش ریسک مربوط به رفتار آنها در سازمان‌ها دارد [۵]. آگاهی از امنیت اطلاعات می‌تواند از تجربه کارکنان در این حوزه حاصل شود. تجربه امنیت اطلاعات منجر به درک، آشنایی، و همچنین توانایی و مهارت برای مدیریت حوادث می‌شود [۳]. لذا سازگاری با خط‌مشی‌ها و رویه‌های امنیت اطلاعات سازمانی به‌عنوان روشی مؤثر برای کاهش نقض امنیت اطلاعات در سازمان‌ها مطرح شده است. به اشتراک‌گذاری دانش امنیت اطلاعات، همکاری در فعالیت‌های امنیتی اطلاعات، مداخله و تجربه با هم شامل جنبه‌های برجسته‌ای از دخالت‌های امنیتی اطلاعات می‌شود و فقط آگاهی را در میان کارکنان افزایش می‌دهد، مدیریت می‌تواند با اشتراک‌گذاری دانش امنیت اطلاعات و با انگیزه‌دادن به کارکنان خود از طریق انگیزه‌های ذاتی و بیرونی این امر را تسهیل کند [۳].

در دو دهه اخیر با ایجاد نگرش استانداردی به امنیت اطلاعات، استانداردهای مفیدی در این حوزه تدوین شده است. می‌توان ISMS را رویکرد ساختار یافته‌ای دانست که چگونگی پیاده‌سازی امنیت اطلاعات را در یک سازمان مشخص می‌کند. به عبارتی با استفاده از فرایند مدیریتی به سمت بهبود مداوم در سازمان حرکت می‌کند، مجموعه ISO/IEC 27000 که تحت عنوان خانواده‌ی استاندارد ISMS شناخته شده است، شامل استانداردهای امنیت اطلاعات است که به‌طور مشترک توسط سازمان بین‌المللی استانداردسازی[2](ISO) وکمیسیون علوم الکترونیکی بین‌المللی [3](IEC) منتشر شده است. استاندارد ISO/IEC27001 که مهم‌ترین و پرمراجعه‌ترین استاندارد در این خصوص است و براساس استاندارد انگلیسی BS7799 و ISO / IEC 17799 ساخته شده است. این آمادگی را فراهم کرده تا الزامات مربوط به ایجاد، پیاده‌سازی، کار، نظارت، تجزیه و تحلیل انتقادی، حفظ و بهبود ISMS را فراهم کند. آخرین نسخه منتشر شده از استاندارد ISO/IEC 27001 نسخه ۲۰۱۳ این استاندارد می‌باشد که ۲ اصلاحیه از آن در سپتامبر ۲۰۱۴ و دسامبر ۲۰۱۵ از سوی سازمان ISO ارائه شده است [۶] و در مارس ۲۰۱۷ نیز آخرین اصلاحیه آن توسط مؤسسه استاندارد انگلستان BSI ارائه گردید که از آن به‌عنوان نسخه بازنگری شده اروپایی این استاندارد یاد می‌شود [۷]. این استاندارد در سراسر جهان توسط همه سازمان‌ها به‌عنوان پایه‌ای برای مدیریت سیاست سازمان و اجرای امنیت اطلاعات مورد استفاده قرار می‌گیرد. این توسط سازمان‌های کوچک، متوسط و بزرگ مورد

1. Information Security Management System

2. International Organization for Standardization
3. International Electrotechnical Commission

استفاده قرار می‌گیرد. در حقیقت، ISO/IEC 27001 به گونه‌ای انعطاف‌پذیر طراحی شده است که توسط هر نوع سازمانی مورد استفاده قرار می‌گیرد. این استاندارد چرخه دمینگ (PDCA)[1] را برای ساختار کلیه فرایندهای ISMS تصویب می‌کند [۸] و هدف از تهیه این استاندارد بین‌المللی، ارائه مدلی است که براساس آن بتوان یک سیستم مدیریت امنیت اطلاعات یا همان ISMS را ایجاد، اجرا، بهره‌برداری، پایش، بازنگری، نگهداری، بهبود و ارتقا بخشید. با در نظر گرفتن مفهوم ریسک‌های کلان کسب و کار سازمان است. استقرار و پیاده‌سازی سیستم مدیریت امنیت اطلاعات در یک سازمان، تحت تأثیر نیازها و اهداف سازمان، الزامات امنیتی، فرایندهای سازمانی به‌کار گرفته شده و اندازه و ساختار سازمان قرار دارد. انتظار می‌رود تمامی این عوامل اثرگذار، در طول زمان دچار تغییر شوند.این یک واقعیت شناخته شده است که سازمان‌ها، در هر دو بخش دولتی و خصوصی، از دوران اسناد به داده‌ها در جریان کسب و کار خود تکامل یافته‌اند [۹]. از دست‌دادن اطلاعات حیاتی سازمان ممکن است موجب از دست رفتن اسرار کسب و کار شود؛ و در مقابل به‌دست‌آوردن اطلاعات حساس خاص می‌تواند موجب افزایش قدرت شود. بنابراین، تغییر این دارایی‌های اطلاعاتی از فیزیکی (به صورت اسناد) به دنیای دیجیتال، جنایتکاران را مجبور می‌کند تا راهبرد حمله خود را برای روند دوباره تنظیم کنند. جرایم سایبری در حال حاضر بیش از موارد سرقت‌های متداول است [۱۰]. روند نشان می‌دهد که دوران جنگ سایبری به سرعت رو به رشد است [۱۱] [۱۲]. بنابراین، اگر کسب و کارها و اقتصادها در مواجهه با این تهدیدات رشد کنند، باید امنیت اطلاعات را جدی بگیرند و در آن سرمایه‌گذاری کنند.

استقرار سیستم مدیریت امنیت اطلاعات در شرکت‌ها و سازمان‌های دولتی به‌عنوان بخشی از طرح جامع فناوری اطلاعات و در راستای اهداف کلان شرکت‌ها و بنا به دستور مدیریت ارشد، صورت می‌پذیرد. سند راهبردی امنیت فضای تولید و تبادل اطلاعات در کشور توسط هیأت‌وزیران و ریاست‌جمهوری در سال ۱۳۸۷ تصویب و به دستگاه‌های ذی‌ربط برای اجرایی‌شدن در راستای برنامه چهارم توسعه ابلاغ شده است [۱]. و با پایشی که در سال ۱۳۹۴ در راستای اهداف کمی برنامه پنجم توسعه صورت گرفته است، ۵۳ درصد دستگاه‌های اجرایی (دستگاه‌های موضوع ماده (۵) قانون مدیریت خدمات کشوری که به استناد ماده (۱۱۷) قانون مذکور مشمول آن قانون هستند.) اقدام به استقرار سامانه مدیریت امنیت اطلاعات (ISMS) نمودند [۲].

یک ابزار، مدل بلوغ امنیت اطلاعات، که جهت پایش سطح امنیت اطلاعات سازمان است. هر وسیله‌ای که با سطوح تکاملی برای ارزیابی قابلیت‌های سیستم‌های اطلاعاتی سازمان برای برآوردن نیازهای امنیتی، درحالی‌که اهداف سازمان در حین حملات امنیتی و حوادث تضمین‌شده است [۱۳]. طبق گفته‌های لون [۱۴]، یک مدل بلوغ دنباله‌ای از سطح بلوغ برای اشیاء خاص، معمولاً افراد، سازمان‌ها یا فرایندها است. در این مدل‌ها مسیر تکاملی، پیش‌بینی شده، مورد نظر یا معمولی، از طریق سطوح گسسته ارائه شده است. علاوه بر موارد فوق، این مدل‌ها معیارهای لازم را برای دستیابی به هر یک از مراحل بلوغ مدل ارائه می‌دهند. بنابراین، مدل‌های بلوغ به ما این امکان را می‌دهند تا ببینیم که در چه مرحله از روند تکاملی برخی اشیاء با هم ملاقات می‌کنند. سطح بلوغ از سطح اولیه ظرفیت پایین‌تر تا سطح پیشرفته متناسب با حداکثر ظرفیت واقعیت مورد نظر سازماندهی می‌شود. برای رسیدن به مراحل بلوغ بالاتر، لازم است که پیشرفت مستمر در توانایی یک شیء معین وجود داشته باشد. بکر و همکاران [۱۵] استدلال می‌کنند که مدل‌های بلوغ ابزارهایی هستند که برای درک و حل مشکل ظرفیت و به‌دست‌آوردن اقدامات بهبودی در خدمت هستند.

TCSEC[2]، ITSEC[3] و CC[4] به‌طور کلی به‌عنوان سیستم‌های ارزیابی در زمینه‌های امنیتی اطلاعات استفاده می‌شوند. در اوایل دهه ۱۹۷۰، وزارت دفاع ایالات‌متحده کار خود را بر روی مجموعه‌ای از الزامات امنیتی رایانه‌های موردنظر برای ارتش آمریکا آغاز کرد. تلاش‌ها در نهایت منجر به معیار ارزیابی امنیت کامپیوتر قابل اعتماد شد که همچنین به‌عنوان "کتاب نارنجی" شناخته می‌شد که رسماً در سال ۱۹۸۳ منتشر شد. نسخه فعلی TCSEC در سال ۱۹۸۵ منتشر شد. از آن به بعد، چندین اسناد دیگر برای تفسیر معیارهای شبکه‌ها و پایگاه‌های داده ارائه شده است. همه این کتاب‌ها اغلب به‌عنوان مجموعه رنگین‌کمان شناخته می‌شوند. ITSEC یک پروژه مشترک از اعضای اتحادیه اروپا از جمله فرانسه، آلمان، هلند و بریتانیا است. بر خلاف TCSEC، ITSEC بطور جدی بین عملکرد و تضمین، صحت و کارآیی اطمینان، جدایی می‌یابد. به منظور ایجاد یک استاندارد بین‌المللی کانادا، فرانسه، هلند، آلمان و ایالات‌متحده در سال ۱۹۹۳ برای بهبود معیارهای ارزیابی موافقت کرده‌اند [۱۶]. در سال ۱۹۸۶، وزارت دفاع آمریکا برای ارزیابی توانایی‌های شرکت‌های نرم‌افزاری که با آنها کار می‌کرد، به روشی نیاز داشت، بنابراین واتس همفری، تیم SEI و شرکت میتر این وظیفه را برعهده داشتند. در سال ۱۹۹۱ نسخه اول، مدل بلوغ CMM[5] از قابلیت‌ها منتشر شد. این مدل برای رسیدن به بهترین تجارب برای ارزیابی و پیاده‌سازی حاکمیت فناوری اطلاعات راهکاری کاربردی و مفید است. این مدل با تبدیل‌شدن به CMMI[6] [۱۷] به موفقیت چشمگیری رسیده است. می‌توان از یک روش مبتنی بر ریسک

1. Plan-Do-Check-Act

2. Trusted Computer System Evaluation Criteria
3. Information Technology Security Evaluation Criteria
4. Common Criteria
5. Capability Maturity Model
6. Capability Maturity Model Integration

برای سنجش و مدیریت ریسک‌های امنیتی در زمینه رسالت و راهبرد کسب و کار بهره برد و برای ساده‌تر کردن تحلیل شکاف امنیتی، از این چارچوب ارزیابی ریسک سایبری بی‌نظیر استفاده نمود [۱۸]. با توجه به موفقیت بدست آمده، اصولی که برای توسعه مدل‌های بلوغ SEI به‌کار رفته است، الهام‌بخش سایر نویسندگان، اعضا دانشگاهیان و دست‌اندرکاران بود، و اکنون صدها مدل برای حوزه‌های مختلف اعمال می‌شود [۶]. در حال حاضر، دو مرجع اصلی مدل‌های بلوغ، CMMI و ISO / IEC 15504 هستند که هر دو مربوط به فرایندهای مهندسی نرم‌افزار هستند. SSE-CMM[1] مجموعه‌ای از بهترین روش‌های مهندسی امنیتی است. SSE-CMM مهندسی امنیتی را به سه حوزه اساسی تقسیم می‌کند: ریسک، مهندسی و تضمین. SSE-CMM دارای دو بعد، دامنه و قابلیت است. بعد دامنه شاید ساده‌تر از بعد قابلیت برای درک باشد. این ابعاد به سادگی شامل تمام شیوه‌هایی است که در مجموع مهندسی امنیتی را تعریف می‌کند. بعد توانایی و قابلیت نشان‌دهنده شیوه‌هایی است که نشان‌دهنده مدیریت فرایند و توانایی نهادینه‌شدن است. این شیوه‌ها به‌عنوان شیوه‌های عمومی نامیده می‌شوند، زیرا در طیف وسیعی از دامنه‌ها کاربرد دارند. SSE-CMM مدل ۵ مرحلهٔ بلوغ را نشان می‌دهد: غیررسمی؛ برنامه‌ریزی و مدیریت؛ تعریف خوب؛ کنترل کمی و بهبود مستمر [۱۹] و مهم‌تر از همه SSE-CMM، ادعا می‌کند راه‌حلی برای کاهش هزینه‌ها با قابلیت‌های بالاتر به ارمغان آورده است [۲۰].

COBIT[2] چارچوبی برای توسعه، پیاده‌سازی، نظارت و بهبود حاکمیت فناوری اطلاعات است. کوبیت از نظر دامنهٔ کار حد واسط پرداختن به چگونگی و چه چیزی است، یعنی نگاه فرایندی و همچنین توجه و تمرکز به اجزاء حاکمیت فناوری اطلاعات را توأمان داراست. توسط انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی (ISACA)[3] ایجاد شده است و از SE-CMM استخراج شده. COBIT2019 جدیدترین تکامل چارچوب کوبیت در سطح جهانی شناخته شده و قدرت کوبیت در وسعت ابزارها، منابع و راهنمایی‌های خود برای حاکمیت و مدیریت شرکت‌های بزرگ IT است [۱۸].

مدل NIST[4] مدل بلوغ مؤسسه ملی استاندارد و فناوری بر روی مستندسازی روش‌ها، نشان‌دهنده فعالیت‌های امنیتی در چرخه حیات سیستم کامپیوتری است که می‌تواند با روش‌های سنتی سیستم اطلاعاتی ترکیب شود. این شامل آغاز، توسعه/ خرید، پیاده‌سازی، بهره‌برداری، نگهداری و دفع است [۱۹]. NIST یک راهنمای خود ارزیابی ارائه داده که یک روش برای تعیین وضعیت فعلی برنامه‌های امنیتی اطلاعات است و در صورت لزوم هدف را برای بهبود ایجاد می‌کند. با استفاده از یک پرسشنامه گسترده‌ای که حاوی اهداف و تکنیک‌های کنترل خاصی است، علیه آن یک سیستم طبقه‌بندی نشده یا گروهی از سیستم‌های متصل می‌تواند آزمایش و اندازه‌گیری شود. مشابه مدل HMG IA[5] بلوغ است. مشابه به این معنی که اول سطح نیازهای امنیتی را برآورده می‌کند و سیاست‌ها را ایجاد می‌کند. دوم، رویه‌ها / فرایندها با توجه به سیاست‌های تعیین‌شده تنظیم می‌شوند. و در سطح سوم به اجرای رویه‌ها / فرایندها و غیره می‌پردازد [۲۱]. مدل بلوغ اطمینان HMG در واکنش به طرح‌های دولت انتقالی و خدمات مشترک، نیاز به اشتراک اطلاعات در میان ادارات دولتی انگلیس ضروری بود. اما مهم‌تر از همه این بود که نیاز به استانداردهای یکنواخت برای اطمینان در مورد اطلاعات به اشتراک گذاشته شده است. در نتیجه، مدل بلوغ اطمینان HMG IA و چارچوب ارزیابی توسعه یافت. این به‌عنوان وسیله‌ای برای ارزیابی و تضمین هر یک از گروه‌های شرکت‌کننده در بلوغ یکدیگر است [۲۲]. سیستم ISM3[6] برای جلوگیری و کاهش حملات، خطاها و حوادثی که امنیت را به خطر می‌اندازند معرفی شد. مدل اطمینان اطلاعات براساس مدل ارزیابی ریسک و پیروی از یک مدل سعی و کوشش بود. این مدل معیار ارزیابی را معرفی می‌کند اما بهترین شیوه‌های امنیتی را ارائه نمی‌دهد [۱۳]. مدل بلوغ را می‌توان برای بهبود یک روند و در نتیجه بهبود کیفیت سیستم‌ها یا محصولات/ خدمات ناشی از فرایند بهبودیافته استفاده کرد. اعتقاد بر این است که کیفیت یک سیستم به شدت تحت تأثیر فرایندی است که برای به‌دست آوردن، توسعه و حفظ آن مورد استفاده قرار می‌گیرد [۲۳]. به‌طور کلی مدل‌های بلوغ امنیت اطلاعات مختلفی در این پژوهش برای بهبود کیفیت و بهبود پردازش نرم‌افزار و مدیریت بررسی و مقایسه شده است [۳,۱۰,۱۹,۲۰,۲۳].

۳- سؤال اصلی این پژوهش

چگونه می‌توان الگوی و مدل بلوغ ویژه ISMS را طراحی کرد که چالش‌های سازمان‌ها و صنایع مختلف را حوزه امنیت اطلاعات هدف قرار دهد؟

۴- بیان مسأله

امروزه امنیت اطلاعات یکی از چالش‌های اصلی در عصر دانایی و اطلاعات محسوب می‌شود و حفاظت از اطلاعات در برابر دسترسی غیرمجاز، تغییرات، خرابکاری و افشا، امری ضروری و اجتناب‌ناپذیر به‌شمار می‌رود. از این‌رو، امنیت دارایی‌های اطلاعاتی، برای تمامی سازمان‌ها امری حیاتی بوده و مستلزم یک مدیریت تأثیرگذار می‌باشد. این موضوع در سال‌های اخیر با بالارفتن تهدیدات و حملات سایبری به سازمان‌ها و روند رو به رشد آن مورد توجه جدی قرار گرفته است. نقض امنیت اطلاعات نه تنها منجر به هزینه‌های اضافی برای سازمان‌ها می‌شود، بلکه آنها نیز به‌طور قابل توجهی تحت تأثیر قرار می‌گیرند. هدف و انگیزه این مقاله به دلیل چالش های پایش اجرای امنیت در سازمان ها بوده است. علاوه بر چالش‌های اجرایی، اجرای بهترین شیوه‌های اجرای امنیت مورد توجه است.

1. Systems Security Engineering Capability Maturity Model
2. Control Objectives for Information and Related Technologies
3. Information Systems Audit and Control Association
4. National Institute of Standards and Technology
5. HMG Information Assurance Standard
6. Information Security Management Maturity Model

۵- روش پژوهش

پژوهش حاضر با هدف پایش بلوغ امنیت اطلاعات و سطح پیاده‌سازی ISMS در واحدهای ستادی شرکت‌های زیرمجموعه صنعت نفت انجام شده است. در ابتدا تمرکز بر روی مطالعه الزامات امنیت اطلاعات مانند استانداردهای امنیت فناوری اطلاعات (ISO/IEC 27001,27002) و پس از آن بررسی مدل‌های بلوغ امنیت اطلاعات از طریق مقالات علمی و پژوهشی بوده است. پس از درک موضوع و چالش اصلی، جامعه آماری پژوهش انتخاب شد که جامعه آماری پژوهش، مدیران و کارشناسان اداره فناوری اطلاعات یکی از مجموعه‌های ستادی صنعت نفت بوده است. پژوهش به صورت روش آمیخته کیفی ـ کمی انجام شده است. به منظور جمع‌آوری داده‌ها در پژوهش حاضر از روش کتابخانه‌ای، مطالعات میدانی، پرسشنامه و مصاحبه استفاده شده است. و مقالات، اسناد، دستورالعمل‌ها و مبانی مربوط به شناسایی چالش‌های امنیت فناوری اطلاعات در این مجموعه ستادی مورد بررسی قرار گرفته و با توجه به آن و از طریق مصاحبه نیمه ساختاریافته، به شناسایی اهداف و ریسک‌های امنیتی و موانع پرداخته شده و بصورت توصیفی مورد تحلیل قرار گرفت تا چالش‌های امنیتی فناوری اطلاعات مشخص گردد. مؤلفه‌های کیفی مؤثر شناسایی شده در قالب پرسشنامه تدوین شد و در اختیار جامعه آماری قرار گرفت و داده‌های لازم بدست آمده است.

در بخش کمی اطلاعات دارایی‌های این شرکت در حوزه شبکه و ارتباطات، سخت‌افزارها، برنامه‌های کاربردی و پایگاه‌های اطلاعاتی، ساختار و سازمان، محیط‌های فیزیکی و کارکنان براساس پرسشنامه‌ها با توجه به استانداردهای امنیت فناوری اطلاعات ISO/IEC ۲۷۰۰۱: ۲۰۰۵ جمع‌آوری شده و مدل ارزیابی بلوغ امنیتی براساس مطالعات قبلی و شرایط موجود انتخاب شده است. این مدل بلوغ امنیت اطلاعات دارای ۵ فاز می‌باشد. مدل بلوغ امنیت اطلاعات به‌عنوان ابزاری جهت ارزیابی توانایی سازمان‌ها برای مطابقت با اهداف امنیت، یعنی، محرمانگی، یکپارچگی و در دسترس‌بودن و جلوگیری از حملات و دستیابی به مأموریت شرکت علی‌رغم حملات و حادثه‌ها می‌باشد با تجزیه و تحلیل داده‌ها براساس مدل نتایج کمی بدست می‌آید. تجزیه و تحلیل داده‌ها با در نظر گرفتن اهداف و راهبردهای کلان کسب و کار و با برآورد ریسک و آسیب‌پذیری‌های دارایی‌ها و احتمال وقوع تهدیدات تخمین زده شده است. همچنین بررسی قوانین، مقررات بالادستی، الزامات کاری و فرهنگ حاکمیتی شرکت در نتایج حاصله مؤثر هستند. و در نهایت ارائه گزارش براساس کلیه مستندات و تجزیه و تحلیل آنها بدست آمده است.

۵-۱- شاخص‌های پایش امنیت اطلاعات براساس استاندارد ISO27001

شاخص‌های پایش در این پژوهش (با توجه به زمان انجام آن) براساس حوزه‌های یازده‌گانه استاندارد ISO/IEC 27001:2005 (مطابق با جدول ۱) تعیین شده است. زیرا مبنای طراحی و پیاده‌سازی سیستم مدیریت امنیت اطلاعات در استانداردها می‌باشد [۲۴]. پس از تعیین معیارهای پایش، جهت گردآوری اطلاعات مورد نیاز، متناظر با هر معیار مجموع پرسش‌هایی طراحی شده است که پاسخگویی به این پرسش‌ها کاستی‌های موجود در سازمان را نمایان می‌سازد و جایگاه امنیت شرکت را مشخص می‌کند.

جدول ۱- معیارها و زیرمعیارهای حوزه‌های امنیت براساس استاندارد ISO/IEC 27001:2005

شماره حوزه	نام حوزه	معیارهای‌های زیرمجموعه هر حوزه
۱	خط مشی امنیت	خط‌مشی امنیت اطلاعات
۲	سازمان امنیت اطلاعات	سازمان داخلی
		طرف‌های خارجی
۳	مدیریت دارایی	مسئولیت دارایی‌ها
		رده‌بندی اطلاعات
۴	امنیت منابع انسانی	پیش از استخدام
		حین خدمت
		خاتمه خدمت یا تغییر سمت
۵	امنیت فیزیکی و محیطی	نواحی امن
		امنیت تجهیزات
۶	مدیریت ارتباطات و عملیات	روش‌های اجرایی و مسئولیت‌های عملیاتی
		مدیریت ارائه خدمت شخص‌ثالث
		طرح‌ریزی و پذیرش سیستم
		محافظت در برابر کدهای مخرب و سیار
		نسخه‌های پشتیبان
		مدیریت امنیت شبکه
		اداره‌کردن رسانه‌های ذخیره‌سازی
		تبادل اطلاعات
		خدمات تجارت الکترونیک
		پایش
۷	کنترل دسترسی	الزامات کسب‌وکار برای کنترل دسترسی
		مدیریت دسترسی کاربر
		مسئولیت‌های کاربر
		کنترل دسترسی به شبکه
		کنترل دسترسی به سیستم عامل
		کنترل دسترسی به برنامه‌های‌کاربردی و اطلاعاتی
		محاسبه سیار و کار از راه دور
۸	اکتساب، بهبود، حفظ و نگهداری سیستم‌های اطلاعاتی	الزامات امنیتی سیستم‌های اطلاعاتی
		پرداش صحیح در برنامه‌های کاربردی
		کنترل‌های رمز نگاری
		امنیت فایل‌های سیستم
		امنیت در فرایندهای بهبود و پشتیبانی
۹	مدیریت استمرار کسب و کار	جنبه‌های امنیت اطلاعات مدیریت استمرار کسب و کار
۱۰	انطباق	انطباق با الزامات قانونی
		انطباق با خط‌مشی‌ها و استانداردهای امنیتی و انطباق فنی
		ملاحظات ممیزی سیستم های اطلاعاتی
۱۱	مدیریت حوادث امنیت اطلاعات	گزارش‌دهی وقایع و ضعف‌های امنیت اطلاعات
		مدیریت رخدادها و بهبودهای امنیت اطلاعات

۵-۲- مدل بلوغ امنیت اطلاعات

مفهوم مدل‌های بلوغ بطور فزاینده‌ای در فیلد سیستم‌های اطلاعاتی به‌عنوان یک رویکرد برای توسعه سازمانی یا به‌عنوان وسیله‌ای برای ارزیابی سازمانی استفاده شده است. هر چارچوب نظام‌مندی برای انجام الگوبرداری و بهبود عملکرد می‌تواند یک مدل باشد و درصورتی‌که دارای فرایندهای بهبود مستمر باشد می‌تواند یک مدل بلوغ باشد. بلوغ، بر سیستمی که بطور شفاف و کامل، کنترل، اندازه‌گیری، مدیریت و تعریف شده است، دلالت دارد. برای شناسایی ضعف‌ها و قدرت‌های امنیتی یک سازمان خاص، مدل‌های مختلفی ارائه شده است. هدف، شناسایی یک فاصله بین تئوری و عمل می‌باشد که می‌تواند از طریق رویکرد فرایندمحور به هم نزدیک شوند. مدل بلوغی که در این پروژه معرفی می‌شود و مورد استفاده قرار می‌گیرد، یک نقطه شروع برای پیاده‌سازی امنیت، یک دیدگاه عمومی از امنیت و یک چارچوب برای اولویت‌بندی عملیات، فراهم می‌سازد. این مدل بلوغ امنیت اطلاعات دارای ۵ فاز می‌باشد که شمای کلی آن در شکل ۱ ارائه شده است.

شکل ۱- شمای کلی مدل بلوغ امنیت اطلاعات

فاز ۱- اعتماد کورکورانه

این حالت نقطه شروع برای هر سازمانی می‌باشد. زمانی‌که سازمان در مورد تهدیداتی که سیستم‌های اطلاعاتی با آن مواجه است آگاه می‌شود، آن سازمان در مرحله اولیه از بلوغ امنیت قرار دارد. سازمان‌ها تهدیدات کسب و کار را به دلیل آسیب‌های موجود تشخیص می‌دهند ولی سیاست و رویه تعریف شده‌ای برای حفاظت از سازمان در دست ندارند. به علاوه سازمان ممکن است که تجربه عملی کمی در پیاده‌سازی سیستم‌های امنیتی داشته باشد. اکثر کنترل‌های پیاده‌سازی شده واکنشی و تدافعی می‌باشند و برنامه‌ریزی شده نیستند. هدف در فاز اعتماد کورکورانه معمولاً بر فعالیت‌های کسب و کارِ سازمان می‌باشد و توجه کمی بر روی امنیت سازمان وجود دارد. اهداف در پاسخ به حملات از طریق پیاده‌سازی بخش‌هایی از امنیت تغییر می‌یابند ولی ادامه‌دار نمی‌باشد.

فاز ۲- شکل‌گیری اولیه

این فاز نشان‌دهنده یک فرایند منظم به سمت امنیت اطلاعات می‌باشد. این سطح از طریق فعالیت‌های مجزا شناخته می‌شود. رویه و سیاست رسمی امنیت اطلاعات وجود ندارد. این وضعیت از طریق آشفتگی، عدم سازگاری بدلیل از دست‌دادن منابع ناشی از حملات، قابل تشخیص می‌باشد. در این مرحله است که تیم امنیتی تشکیل می‌شود و تیم امنیتی به درستی در مورد نقش‌ها و مسئولیت‌هایشان آگاه می‌شوند. با تشکیل تیم امنیتی، افراد تیم، دیگر کارکنان سازمان را از تهدیدات و حوادث امنیتی که آنها را تهدید می‌کند، آگاه می‌سازند. در این مرحله فرایندها و استانداردهای امنیت اطلاعات بصورت غیررسمی تعریف می‌شود، اما بطور منظم و دقیق مورد اجرا و بررسی و بازبینی قرار نمی‌گیرند. در این مرحله هیچ برنامه امنیتی به‌طور رسمی معرفی نمی‌گردد و مستندی برای راهنمایی امنیتی تدوین نشده است و بیشتر بصورت شفاهی و غیررسمی می‌باشد.

فاز ۳- استقرار

این وضعیت نقطه آغاز برای سازمان‌هایی می‌باشد که می‌خواهند از سرمایه‌گذاری‌های خود محافظت کنند و از استمرار آن مطمئن باشند. امنیت شبکه و برنامه‌های کاربردی پیاده‌سازی شده است ولی تغییرات به صورت مرکزی مدیریت نشده است و درخواست‌های امنیتی تک منظوره و مجزا رایج می‌باشد. در این حالت، سازمان‌ها به تعاملات بین کاربر و سیستم اعتماد می‌کنند. برنامه‌های آگاهی امنیتی تنها برای منابع کلیدی مورد توجه قرار می‌گیرد. فرایند اساسی اکثر سیستم‌ها تعامل بین سیستم و کاربر است. به همین دلیل، این تعامل بزرگ‌ترین تهدید می‌باشد. سازمان‌ها، کاربرانشان را به‌عنوان تهدید و خطر برای سیستم‌های خود دسته‌بندی نمی‌کنند. عملکرد کاربران می‌تواند نقطه آغازی برای برخی حملات باشد. اهداف این مرحله معمولاً بر روی فعالیت‌های کسب و کارِ سازمان و محافظت از سیستم‌های اصلی و هسته‌ای متمرکز می‌باشد. معمولاً، یک سازمان، امنیت یک سیستم را بعد از پیاده‌سازی آن مورد توجه قرار می‌دهد. دو محدودیت در این مرحله وجود دارد: اول، محدودیت مالی و هزینه‌کردن بر روی سیستم‌هایی که ارزش افزوده‌ای برای ورودی کسب و کار ندارند. دوم، سازمان‌ها سرمایه‌گذاری‌های اولیه خود را در حوزه امنیت خاتمه‌یافته قلمداد می‌کنند. در سازمان درصدی وجود دارد که نشان می‌دهد سیستم‌های آن‌ها حافظت شده می‌باشد درصورتی‌که آن‌ها از خطرات و آسیب‌ها بی‌اطلاع هستند.

فاز ۴- نهادینه‌سازی

این وضعیت از طریق مدیریت مرکزی تمام مسائل و سیاست‌های مرتبط با امنیت شناخته می‌شود. کاربران مورد اعتماد می‌باشند ولی تعامل آن‌ها با سیستم به‌عنوان یک تهدید دیده می‌شود. تغییرات مجزایی وجود ندارد و مدل‌های پیکربندی مرکزی که تمام پیکربندی‌ها را هدایت می‌کنند، پیاده‌سازی شده است. رویه‌ها و سیاست‌های امنیتی در یک جایگاه مشترک با یکدیگر با مکانیزم‌های تحویل مناسب برای مساعدت به آگاهی و سازگاری قرار دارند. کنترل دسترسی‌ها الزامی می‌باشد و مورد نظارت قرار می‌گیرد. به‌طور کلی، اهداف این سطح، متمرکز بر فعالیت‌های کسب و کار، کاربران و مانیتورکردن تهدیدات امنیتی و تمام وصله‌هایی است که تست و پیاده‌سازی شده‌اند، است. معمولاً، سازمان‌ها در این حالت در مورد نیازهای امنیتی خود آگاه می‌باشند و بر روی سیستم‌هایی که از سازمان محافظت می‌کنند سرمایه‌گذاری می‌کنند.

فاز ۵- نگهداری و بهبود مستمر

این وضعیت با داشتن کنترل بر روی نیازهای امنیتی سازمان، مانیتورکردن سیستم‌ها، آگاه‌بودن از تهدیدات و ارزیابی از طریق مقایسه سازمان با دیگر سازمان‌ها و استانداردهای بین‌المللی مشخص می‌شود. به‌علاوه، یک وظیفه امنیتی جامع ایجاد شده است که هم کارآمد و هم به‌صرفه می‌باشد و پیاده‌سازی با کیفیت بالا را ارائه می‌کند. این طرح جامع دارای سیاست‌ها و رویه‌های رسمی برای جلوگیری، شناسایی و اصلاح مسائل و مشکلات مرتبط با امنیت است. حاکمیت سازمان، سیاست‌هایی برای ممیزی داخلی دارا می‌باشد که مستقل بوده و فعالیت‌های عینی برای اضافه‌کردن ارزش و بهبود امنیت سازمان طراحی شده است. نتایج هر فعالیت ممیزی منتشر و عملیات، پیاده‌سازی شده است. در سازمان باید برای رسیدن به نگهداری و بهبود مستمر، امنیت رویدادها و ملاحظات امنیتی در یک مسیر نظام‌مند دنبال شوند. سازمان باید سیاست‌های رسمی مناسب و طرح‌های کسب و کار مؤلفه‌هایی برای امنیت داشته باشند. استفاده از فناوری‌های خاص در سرتاسر سازمان به‌صورت یکنواخت و پیاده‌سازی از یک طرح کسب و کار بوجود می‌آید. این فاز همچنین معماری امنیت را در یک سازمان مورد بررسی قرار می‌دهد. یک سیستم برای ارائه قابلیت ردیابی در سرتاسر سازمان ایجاد شده است. برای مدیریت امنیت، سیاست‌ها در این فاز، کنترلیِ پیشگیرانه، تشخیصی و اصلاحی می‌باشند.

۶- پایش اجرای امنیت اطلاعات در سازمان با بهره‌مندی از مدل بلوغ امنیتی در اداره IT یکی از شرکت‌های زیرمجموعه صنعت نفت در ایران

امروزه با به‌کارگیری گسترده از خدمات فناوری اطلاعات در سازمان‌های مختلف از جمله شرکت‌های نفتی، می‌توان گفت که اغلب سازمان‌ها با یکی از حوادث و یا مشکلات امنیت اطلاعات نظیر آلودگی به ویروس‌ها و نرم‌افزارهای مخرب، دسترسی غیرمجاز افراد بدون صلاحیت به داده‌های حساس سازمان، قطعی و یا کندی شبکه‌های اطلاعاتی، عدم تطابق و صحت اطلاعات در برنامه‌های کاربردی و غیره مواجه بوده‌اند. سازمان‌ها و شبکه‌ها و سیستم‌های اطلاعاتی آن‌ها به صورت فزاینده‌ای با تهدیدهای امنیتی با منشأهای متنوع شامل کلاه‌برداری از طریق کامپیوتر، جاسوسی، کارشکنی، خرابکاری، آتش‌سوزی و سایر بلایای طبیعی رودررو هستند. امنیت اطلاعات فراتر از نصب یک نرم‌افزار ضد ویروس و یا پیکره‌بندی یک دیواره آتش یا حتی نصب سیستم‌های تشخیص و پیشگیری از نفوذ می‌باشد. معمولاً در پروژه‌های توسعه سیستم‌ها تمایل زیادی برای نادیده‌گرفتن و صرف‌نظرکردن از نیاز به مدل‌سازی نیازهای امنیتی دیده می‌شود که شامل خط‌مشی امنیتی نیز می‌شود [۲۵]. اطلاعات به‌عنوان دارایی با ارزش نیازمند امنیت یا حفاظت است. حفظ امنیت اطلاعات، یکپارچگی اطلاعاتی و پردازشی و نیز در دسترس‌بودن آنها برای شرکت ملی نفت ایران و شرکت‌های زیرمجموعه ضروری و حیاتی می‌باشد. بسیار مقرون به صرفه و کارآمدتر است که نیازهای امنیتی، در مرحله طراحی و برنامه‌ریزی چرخه عمر تولید سیستم‌های مرسوم جهت‌دهی شوند. پیاده‌سازی و حفظ امنیتی که بعد از اجرای طرح اعمال شود ناکارآمدتر و هزینه برتر از نمونه از پیش طراحی شده آن است [۲۶]. لذا در یکی از شرکت‌های زیرمجموعه صنعت نفت که قصد استقرار سیستم مدیریت امنیت اطلاعات را در سال‌های ۹۱ الی ۹۲ داشتند با عنایت

به اهمیت ضرورت سیستم مدیریت امنیت اطلاعات به بررسی نتایج بدست آمده از چک‌لیست‌های ارزیابی امنیتی شرکت و همچنین مدل بلوغی که برگرفته از مدل‌های بلوغ سازمان‌ها و صنایع مختلف می‌باشد پرداختیم [۳,۱۰,۱۹,۲۰,۲۳]. در این بخش با استفاده از نگاشت اطلاعات کسب‌شده و مدل بلوغ امنیت اطلاعات ارائه‌شده، جایگاه شرکت در این مدل بومی بلوغ مورد بررسی قرار گرفت. درصد پیاده‌سازی حوزه‌های یازده‌گانه کنترلی ISO/IEC ۲۷۰۰۱: ۲۰۰۵ در جدول ۲ ارائه شده است.

جدول ۲- درصد پیاده‌سازی حوزه‌های یازده‌گانه کنترلی ISO 27001 در شرکت

حوزه‌های یازده‌گانه ISO۲۷۰۰۱	درصد پیاده‌سازی
خط مشی‌های امنیتی	٪۰
سازمان امنیت اطلاعات	٪۱۸
مدیریت دارایی	٪۱۵
امنیت منابع انسانی	٪۳۵
امنیت فیزیکی و محیطی	٪۵۲
مدیریت ارتباطات و عملکرد	٪۶۵
کنترل دسترسی	٪۷۶
اکتساب، بهبود، حفظ و نگهداری سیستم‌های اطلاعاتی	٪۵۳
مدیریت رخدادهای امنیت اطلاعات	٪۵۷
مدیریت استمرار کسب و کار	٪۵۰
انطباق	٪۴۱

در ادامه وضعیت هر یک از این حوزه‌های کنترلی در شرکت مورد تحلیل و بررسی قرار گرفت.

کنترل اول، خط‌مشی‌های امنیتی، هدف این کنترل، ارائه دستورالعمل مدیریت و حمایت از امنیت اطلاعات براساس الزامات کسب و کار و قوانین و مقررات مربوطه است. سند خط‌مشی امنیت اطلاعات باید توسط مدیریت به تأیید برسد و پس از انتشار به کلیه کارمندان و اشخاص بیرونی ذی‌نفع ابلاغ گردد. براساس درصدهای بدست‌آمده، در شرکت خط‌مشی امنیت اطلاعات تدوین نشده است و رویه و دستورالعمل رسمی در این زمینه وجود ندارد و اکثر کنترل‌ها و دستورالعمل‌ها بصورت شفاهی بوده و بصورت مکتوب و منظم وجود ندارد.

در کنترل دوم، سازمان امنیت اطلاعات، درصد پیاده‌سازی حدود ۱۸ درصد برآورد شده است. در این کنترل، سازمان باید هم از نظر داخلی و هم از نظر طرف‌های بیرونی ملزم به رعایت امنیت اطلاعات گردد. متأسفانه سازمان در این بخش عملکرد ضعیفی دارد. امنیت در مورد طرف‌های بیرونی تقریباً رعایت نشده است. کنترل‌ها در رابطه با گروه‌های بیرونی که به مراکز پردازش اطلاعات دسترسی دارند فقط در قالب قرارداد است و نهایتاً حضور کارمندان سازمان در کنار افراد بیرونی هنگام کار با سیستم می‌باشد. تعهد مدیریت در سطح بالایی قرار نداشته و جلسات پیرامون امنیت در موارد خاص و ضروری برگزار می‌شود. امنیت اطلاعات و پیاده‌سازی آن بطور منظم بازبینی نمی‌شود.

هدف کنترل سوم، مدیریت دارایی، تأمین محافظت از دارایی‌های سازمان و حصول اطمینان از محافظت از دارایی‌ها در یک سطح مناسب است. درصد پیاده‌سازی برای این قسمت حدود ۱۵ درصد برآورد شده است. در این زمینه فقط اموالی که دارای کد مخصوص شرکت هستند، لیست شده‌اند، مالک اموال مشخص نمی‌باشد و به تبع آن کنترلی از سوی مالک اموال انجام نمی‌شود. اطلاعات از لحاظ محرمانگی طبقه‌بندی نشده‌اند و اطلاعات نه در سطح داخل و نه در سطح خارج سازمان برای اشتراک اطلاعات برچسب‌گذاری نشده‌اند. در مجموع این بخش از درصد پایینی برخوردار است و باید مورد توجه بیشتر مدیران مربوطه قرار گیرد.

کنترل چهارم، امنیت منابع انسانی، به لزوم امنیت منابع انسانی در تمام دوران خدمت یک نیرو پرداخته است. در این بخش کنترل‌های مربوط به خاتمه خدمت بهتر رعایت شده است ولی در مورد حین خدمت و تغییر شغل کنترل‌های مناسبی بکار گرفته نمی‌شود و احتمال سوءاستفاده افراد از اطلاعات و منابع شرکت وجود دارد و نظارت به درستی انجام نمی‌شود. درصد پیاده‌سازی در این بخش حدود ۳۵ درصد برآورد شده است.

هدف کنترل پنجم، امنیت فیزیکی و محیطی، جلوگیری از دسترسی غیرمجاز به دارایی‌های سازمان و جلوگیری از ایجاد وقفه در فعالیت‌های سازمان می‌باشد. در این زمینه کنترل‌ها توسط واحدهای حراست، HSE[1] و فناوری اطلاعات انجام می‌شود. هر واحد بطور مجزا مسئول محافظت از دارایی‌ها و پایگاه داده‌های خود می‌باشد. در این بخش نیز ضعف مشخص نبودن مالک دارایی‌ها و اطلاعات و همچنین فقدان طبقه‌بندی اطلاعات به چشم می‌خورد. به دلیل مرکزی‌بودن یکی از ساختمان‌ها، از تجهیزات و ساختمان بصورت قابل‌قبولی محافظت می‌شود گرچه در برخی زمینه‌ها مانند تجهیزاتی که توسط کاربران وارد ساختمان می‌شود یا از آن خارج می‌شود کنترل‌های کافی صورت نمی‌گیرد. درصد پیاده‌سازی که برای این بخش برآورد شده است حدود ۵۲ درصد می‌باشد که تقریباً قابل قبول می‌باشد ولی در این بخش باید کنترل‌های امنیتی بیشتری پیاده‌سازی گردد.

کنترل ششم، مدیریت ارتباطات و عملکرد، هدف از این بخش جلوگیری از خارج‌شدن دارایی‌ها بدون مجوز از سازمان، رعایت توافق‌نامه‌های ارائه خدمات به اشخاص ثالث، اجرا و حفظ سطح مناسبی از امنیت اطلاعات، به حداقل رساندن ریسک خرابی‌های سیستم است، حفاظت در برابر کدهای مخرب و سیار، حفظ تمامیت و درستی و در دسترس‌بودن اطلاعات، حصول اطمینان از اطلاعات موجود در شبکه‌ها، حفاظت از زیرساخت‌های پشتیبانی، توانایی در اداره‌کردن محیط‌های ذخیره‌سازی برای جلوگیری از افشاء غیرمجاز اطلاعات، حفظ امنیت برای تبادل اطلاعات و در نهایت حصول اطمینان از امنیت خدمات تجارت الکترونیک و استفاده ایمن از آن‌ها می‌باشد. در این زمینه نیز کاستی‌هایی به‌خصوص در زمینه‌های پایش

1. Health and Safety Executive

کاربرد سیستم، اطلاعات قابل دسترس عموم، تراکنش‌های برخط، انتقال محیط‌های ذخیره‌سازی فیزیکی، امحای محیط‌های ذخیره‌سازی و مدون‌سازی روش‌های اجرایی عملیاتی وجود دارد که باید مورد توجه مدیران عالی سازمان و مدیران مربوطه قرار گیرد. درصد پیاده‌سازی برای این بخش ۶۵ درصد برآورد شده که درصد مناسبی است.

در کنترل هفتم، کنترل دسترسی، هدف، کنترل‌نمودن دسترسی به اطلاعات می‌باشد. این حوزه در سطح قابل قبولی توسط سازمان رعایت می‌شود و درصد پیاده‌سازی حدود ۷۶ درصد برآورد شده است؛ نقاط ضعفی هم وجود دارد که در ادامه بیان می‌شود. خط‌مشی کنترل دسترسی موجود است اما مدون نمی‌باشد، حقوق دسترسی کاربران در زمان‌بندی‌های مشخص کنترل نمی‌شود، مسئولیت‌های کاربران برای کاهش خطر دسترسی غیرمجاز به صورت خط‌مشی مدون شده وجود ندارد، کاربران از شیوه‌های صحیح انتخاب کلمه عبور استفاده نمی‌کنند، خط‌مشی میزپاک و صفحه پاک رعایت نمی‌شود، کیفیت کلمات عبور بررسی نمی‌گردد، محدودیت‌های زمانی برای استفاده از برنامه‌های کاربردی وجود ندارد (در صورت لزوم اعمال می‌گردد)، خط‌مشی برای محافظت در برابر ریسک‌های بکارگیری امکانات ارتباطات سیار و نیز خط‌مشی برای عملیات کار از راه دور وجود ندارد.

در کنترل هشتم، اکتساب، بهبود، حفظ و نگهداری سیستم‌های اطلاعاتی، هدف، ایجاد الزامات مربوط به کنترل‌های امنیتی، تعیین اعتبار داده‌های خروجی و برنامه‌های کاربردی، حصول اطمینان از امنیت فایل‌های سیستم، امنیت کاربری اطلاعات و نرم‌افزار سیستم، جلوگیری از نشت هرگونه اطلاعات و توسعه نرم‌افزارهای برون‌سپاری شده که توسط سازمان باید نظارت و پایش شوند، است. کاستی‌های موجود در سازمان در ارتباط با این کنترل، عدم توافق و مستندسازی الزامات امنیتی یک پروژه، عدم تعیین مشخصات و تحلیل الزامات امنیتی، عدم نگهداری امن نتایج کنترل‌های پردازش درونی، عدم وجود خط‌مشی‌های کنترل برای رمزنگاری، عدم وجود سیستم مدیریت کلید، عدم وجود کامل رهنمودهایی برای کنترل تغییرات، در نظر نگرفتن ریسک نرم‌افزارهای پشتیبانی نشده، عدم کنترل مناسب بر روی محیط‌های پروژه و پشتیبانی، عدم پیشگیری از فرصت‌های نشت اطلاعات، عدم وجود مدیریت آسیب‌پذیری فنی می‌باشد که باید مورد توجه قرار گیرد. درصد پیاده‌سازی که برای این کنترل برآورد شده است حدود ۵۳ درصد می‌باشد که تقریباً درصد مناسبی است اما باید با پیاده‌سازی کنترل‌های مورد نیاز این درصد ارتقاء یابد.

کنترل نهم، مدیریت رخدادهای امنیت اطلاعات، هدف این کنترل، حصول اطمینان از اقدامات اصلاحی به موقع و همچنین استفاده از یک رویکرد مؤثر و یکنواخت برای مدیریت حوادث امنیت اطلاعات می‌باشد. کاستی‌های سازمان در ارتباط با این کنترل، عدم اطلاع‌رسانی به کاربران شخص ثالث از رویه‌های گزارش وقایع و ضعف‌های تأثیرگذار بر دارایی‌های سازمان، عدم وجود رویه رسمی برای گزارش‌دهی وقایع امنیت اطلاعات، عدم وجود فرایند بهبود مداوم برای واکنش، کنترل، ارزیابی و مدیریت رخدادهای امنیت اطلاعات و عدم در نظر گرفتن تأثیر رخدادهای امنیتی بر هزینه‌ها می‌باشد. درصد پیاده‌سازی این کنترل در سازمان حدود ۵۷ درصد برآورده شده است که درصد نسبتاً مناسبی برای این کنترل می‌باشد.

هدف کنترل دهم، مدیریت استمرار کسب‌وکار، محافظت از فرایندهای کاری حیاتی در برابر رخدادهای امنیتی و خنثی‌سازی هرگونه وقفه در فرایندهای کاری می‌باشد. از جمله مواردی که در این بخش باید مورد توجه قرار گیرد ولی در سازمان مورد قصور واقع شده است، وجود طرح‌های استمرار در برگیرنده امنیت اطلاعات، وجود طرح‌ریزی استمرار کسب‌وکار، حفظ و نگهداری و ارزیابی مجدد طرح‌های استمرار کسب و کار می‌باشد. درصد پیاده‌سازی برای این کنترل حدود ۵۰ درصد برآورد شده است.

هدف کنترل یازدهم، انطباق، جلوگیری از نقض هر یک از قوانین و تعهدات قانونی، قراردادی و الزامات امنیتی و حصول اطمینان از انطباق سیستم‌ها با استانداردها و خط‌مشی‌های امنیتی و افزایش اثربخشی و به حداقل رساندن تداخلات ناشی از فرایندهای ممیزی سیستم‌های اطلاعاتی می‌باشد. کاستی‌های این کنترل که در سازمان باید مورد توجه قرارگیرند، عبارتند از: عدم وجود کنترل‌های خاص برای رعایت آیین‌نامه‌ها (مستقل شده است ولی مدون نمی‌باشد)، عدم وجود روش‌های اجرایی مناسب برای رعایت حقوق مالکیت فکری و حقوق انحصاری در سازمان، عدم وجود خط‌مشی برای محافظت از داده‌ها و حریم خصوصی اطلاعات شخصی، عدم استفاده از مشاوره قانونی برای تضمین انطباق با قوانین ملی، عدم انطباق با خط‌مشی و استانداردهای امنیتی و انطباق فنی، عدم وجود کنترل‌های ممیزی سیستم‌های اطلاعاتی. درصد پیاده‌سازی برای این بخش حدود ۴۱ درصد است.

برای تعیین جایگاه سازمان در مدل بلوغ امنیت اطلاعات باید نگاشتی بین اطلاعات بدست آمده از چک‌لیست‌ها و مصاحبه و سطوح مدل بلوغ صورت گیرد. با توجه به اینکه در شرکت مذکور، ضرورت به‌کارگیری امنیت اطلاعات در سازمان توسط مدیران عالی درک شده است، اقداماتی در زمینه امنیت محیط فیزیکی، شبکه و کامپیوترهای شخصی و کنترل‌های دسترسی و رمزنگاری صورت گرفته است، کمیته‌ی امنیتی متشکل از مدیران عالی سازمان شکل گرفته است، وظایف کارکنان امنیت به خوبی تعریف شده است و وظایف با توجه به توانمندی‌های افراد به آن‌ها سپرده می‌شود، سازمان در مورد تهدیداتی که سیستم‌های اطلاعاتی با آن مواجه می‌باشد تا حدودی آشنایی دارد، در نتیجه جایگاه سازمان از فاز ۱ یعنی فاز اعتماد کورکورانه بالاتر می‌باشد از سویی دیگر، خط‌مشی‌ها و دستورالعمل‌ها بصورت رسمی، مدون و مکتوب موجود نمی‌باشد، برنامه امنیت راهبردی در سازمان پیاده‌سازی نشده است، کنترل‌های امنیتی بصورت واضح و شفاف تعریف نشده است، اعتمادی به تعامل کاربر با سیستم وجود ندارد و نظارت بر اعمال کاربران بصورت محدود انجام می‌شود، فرایندهای امنیتی بخوبی تعریف نشده است و بصورت مکتوب و

مدون موجود نمی‌باشد، برنامه‌های آگاهی‌رسانی بصورت محدود و در موارد ضروری انجام می‌شود، عملیات امنیتی بیشتر بصورت تک منظوره انجام می‌شود که در برخی موارد بصورت برنامه‌ریزی شده بوده و در برخی موارد دیگر بصورت واکنشی و در صورت وقوع یک حادثه امنیتی صورت می‌گیرد. در نتیجه با توجه به اینکه شرکت برخی از خصوصیات و ویژگی‌های سطح ۳ بلوغ مانند برنامه راهبردی امنیت را ندارد، از طرفی برخی مشخصه‌های فاز ۳ مانند رویه‌های امنیتی فناوری اطلاعات بصورت غیررسمی و همچنین اکثر مشخصه‌های فاز ۲ مدل بلوغ را دارا می‌باشد، با بررسی‌ها و تحلیل‌های انجام شده، جایگاه شرکت در مدل بلوغ امنیت اطلاعات بین فاز ۲ (شکل‌گیری اولیه) و فاز ۳ (استقرار) است و به بیان دیگر شرکت در حال گذار از سطح ۲ به سطح ۳ بلوغ می‌باشد.

۷- نتیجه‌گیری

یکی از دغدغه‌ها در سیستم مدیریت امنیت اطلاعات، اجرایی‌شدن واقعی و عملیاتی سیستم و تداوم مؤثر آن در سازمان است. هدف این مقاله ارائه یک مدل بلوغ امنیتی برای فرایند ISMS براساس استاندارد ISO / IEC 27001 است. که می‌توان از آن برای تحلیل و ارزیابی نقاط قوت و ضعف فعلی فرایند ISMS استفاده شود. همچنین می‌توان از آن برای تهیه نقشه راه به سمت پیشرفت تکاملی عملکرد مدیریت امنیت اطلاعات در مورد قابلیت‌های آن و کارایی آن استفاده کرد. به‌طور کلی برای پیاده‌سازی سیستم مدیریت امنیت اطلاعات در یک سازمان، سرمایه‌گذاری بدون هدایت مناسب و پشتیبانی نگرش انسانی هنوز ممکن است یک سرمایه‌گذاری ناپایدار باشد. کنترل‌های فناورانه خوب تنها بدون داشتن الزامات امنیتی مناسب و حمایت مدیران عالی میسر نیست. این سند تحقیق می‌تواند مبنایی برای یک پروژه فنی برای ایجاد یک ابزار واقعی ISMS مبتنی بر وب باشد. و از آنجایی‌که این مدل فقط بر "چگونگی" اجرای صحیح کنترل‌های امنیتی اطلاعات برای دستیابی به وضعیت قابل قبول امنیت اطلاعات و اطمینان از اجرای کلیه اقدامات جهت محافظت از آنها در برابر تهدیدات احتمالی متمرکز شده است، می‌توان از چارچوب COBIT برای کمک به سازمان‌ها در مورد "آنچه" باید انجام شود، بهره برد.

براساس پایش به‌عمل آمده، عوامل مؤثری در اثربخشی سیستم مدیریت امنیت اطلاعات در شرکت‌های زیرمجموعه صنعت نفت شامل موارد ذیل است:

- تعهد مدیران ارشد به سازمان امنیت
- تعریف مناسب قلمروی پروژه ISMS در سازمان
- پیاده‌سازی صحیح و کامل سیاست‌های امنیتی
- تعامل با رویه‌های مدیریت خدمات فناوری اطلاعات (ITSM)[1]
- بلوغ فناوری اطلاعات در سازمان
- رعایت ملاحظات مربوط به نیروی انسانی
- ممیزی دوره‌ای
- پیاده‌سازی به موقع و مناسب طرح‌ها
- ارتباط با سازمان‌ها و نهادهای امنیتی
- امنیت شخص ثالث
- مدیریت صحیح ریسک
- طراحی سیستم مواجهه با بحران

با توجه به موارد مطرح‌شده، استقرار سیستم مدیریت امنیت اطلاعات به‌عنوان سامانه‌ای جامع که همه ابعاد امنیت از جمله خط‌مشی امنیتی، سازمان‌دهی امنیت اطلاعات، مدیریت دارایی‌ها، امنیت منابع انسانی، امنیت فیزیکی و محیطی، مدیریت ارتباطات و عملیات، کنترل دسترسی، استفاده، توسعه و نگهداری سامانه‌های اطلاعاتی، پشتیبانی حوادث، مدیریت تداوم کسب و کار، سازگاری با الزامات قانونی، حقوقی و قراردادی را در برگیرد، در صنعت نفت امری ضروری است. بایستی توجه کرد که امنیت یک فرهنگ است قبل از آنکه یک فناوری باشد. بر این اساس پیاده‌سازی مدیریت امنیت اطلاعات قبل از خرید تجهیزات امنیتی توصیه می‌گردد. وقتی امنیت به صورت فرهنگ نباشد زمان زیادی لازم است تا به صورت یک فرهنگ ایجاد شود و جا بیفتد. امنیت تداوم می‌خواهد. حتی اگر موفق شویم در یک سازمان سیستم مدیریت امنیت را پیاده‌سازی نموده و گواهی استاندارد مربوطه را هم در یک مرحله اخذ نماییم؛ عدم تداوم آن هیچ آورده‌ای را از نظر امنیتی برای سازمان نخواهد داشت. بنابراین همیشه در استانداردهای بین‌المللی از چرخه دمینگ یا PDCA که یک چرخه مدور و دائمی است برای طراحی، انجام، آزمایش و اعمال مجدد طراحی استفاده می‌شود. که لازمه سامانه‌ای اثربخش در سازمان‌های مجموعه صنعت نفت خواهد بود.

۸- محدودیت‌ها

محدودیت‌هایی در این مطالعه وجود دارد. نمونه‌ها از یکی از شرکت‌های زیرمجموعه صنعت نفت جمع‌آوری شده است. یکی از محدودیت‌ها، کمبود شرکت‌هایی است (به‌خصوص در زیرمجموعه صنعت نفت) که سیاست‌های امنیتی اطلاعات را ایجاد کرده‌اند تا ریسک نقض اطلاعات در مؤسسات خود را کاهش دهند. این یک وظیفه سخت برای کسب اجازه از سازمان‌ها و شرکت‌ها برای نظرسنجی‌ها و جمع‌آوری داده‌ها در حوزه امنیت اطلاعات است. با این حال، تعمیم‌یافته‌ها می‌تواند با یک نمونه بزرگ‌تر و شرکت‌های بیشتری برای تحقیق بهبود یابد.

۹- مراجع

۱- هیأت‌وزیران, تصویب‌نامه. "تصویب‌نامه درخصوص تعیین سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور." مرکز پژوهش‌های مجلس شورای اسلامی ایران. ۱۳۸۷.
۲- سازمان فناوری اطلاعات ایران، "سامانه مدیریت امنیت اطلاعات دستگاه‌های اجرایی." درگاه پایش جامعه اطلاعاتی جمهوری اسلامی ایران. ۱۳۹۴.

1. Information Technology Service Mmanagement

3- Nader, Sohrabi Safa, Rossouw Von Solms, and Steven Furnell. "Information security policy compliance model in organizations." Elsevier (computers & security 56 (2016)), 2015: 1-13.
4- Werlinger, Rodrigo, and and et al. "Security Practitioners in Context:Their Activities and Interactions withOther Stake holders within Organizations." International Journal of Human-Computer Studies, 2009: 584-606.
5- Arachchilage, Nalin Asanka Gamagedara, and and et al. "Phishing threat avoidance behaviour: An empirical investigation." Elsevier (Computers in Human Behavior 60 (2016)), 2015: 185-197.
6- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, 2013.
7- bsi. (2017). Available at: https://www.bsigroup.com/en-VN/ISOIEC-27001-Information-Security/
8- Proença, D., & Borbinha, J. (2018, June). Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001. In Business Information Systems (pp. 102-114). doi:10.1007/978-3-319-93931-5_8
9- Rosenzweig, Roy . "Scarcity or Abundance? Preserving the Past in a Digital Era." The American Historical Review, 2003: 735–762.
10- Anderson, Ross, et al. "Measuring the Cost of Cybercrime." The Economics of Information Security and Privacy, October 2013: 265-300.
11- PERLROTH, NICOLE. Hackers in China Attacked The Times for Last 4 Months. TECHNOLOGY, New York: The New York Times Company, JAN. 30, 2013.
12- SANGER, DAVID E. In Cyberspace, New Cold War. New York: The New York Times Company, FEB. 24, 2013.
13- Saleh, Malik F. "Information Security Maturity Model." International Journal of Computer Science and Security (IJCSS), July / August 2011: 316 - 337 .
14- H. van Loon, "Process Assessment and Improvement: A Practical Guide," Jan. 2015.
15- 16. J. Becker, R. Knackstedt, J. Pöppelbuβ, "Developing maturity models for IT management: A procedure model and its application," Business and Information Systems Engineering, Vol. 3, pp 213-222, 2009
16- "https://www.commoncriteriaportal.org/ccra/." https://www.commoncriteriaportal.org/. 2005.
17- CMMI Product Team, "CMMI for Development, Version 1.3," Carnegie Mellon Univ., no. November, p. 482, 2010.
18- https://www.isaca.org/resources/cobit. (2020). Retrieved from ISACA.
19- Xiao-yan, Ge, Yuan Yu-qing, and Lu Li-lei. "An Information Security Maturity Evaluation Model." 2011 International Conference on Advances in Engineering. Procedia Engineering, 2011. 335-339.
20- Hefner, R. and Monroe." System security engineering capability maturity model." Software Process Improvement. 1997.
21- Johnson, L A, Kelley L Dempsey, Ronald S, and Ross S. "https://www.nist.gov/publications/guide-security-focused-configuration-management-information-systems." https://www.nist.gov/. August 12, 2011.
22- Office, Cabinet, and National security and intellige. "https://www.gov.uk/government/publications/hmg-personnel-security-controls." https://www.gov.uk/. April 1, 2013.
23- Wiley, John, and Sons. Capability Maturity Model® Integration (CMMI), Version 1.1--Continuous Representation. Technical, Carnegie Mellon University, 05 February 2002.
24- ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems – Requirements, 2005.
25- Freeman, J.W., Neely, R.B., & Heckard, M.A. "A Validated Security Policy Modeling Approach." Proceedings of the 10th Annual Computer Security Applications Conference, Orlando, FL, 189-200., (1994).
26- Bruce, Glen, & Dempsey, Rob. "Security in Distributed Computing: Did You Lock the Door?" Upper Saddle, River, NJ: Prentice Hall PTR, Prentice-Hall, Inc., (1997)