Critical Success Factors in implementing information security governance (Case study: Iranian Central Oil Fields Company)

Fatemeh Akhavan[1] - Seyed Abdullah Amin Mousavi*[2]
Abolghasem Sarabadani[3]

Abstract

The oil industry, as one of the main industries of the country, has always faced cyber attacks and security threats. Therefore, the integration of information security in corporate governance is essential and a governance challenge. The integration of information security and corporate governance is called information security governance. In this research, we identified "critical success factors" in the implementation of information security by using metasynthesis method and studying sources related to information security. Because before any planning and policy making in the field of information security governance, it is necessary to pay attention to this category. In the following, we classified these factors based on the focus areas of information security governance, which include strategic alignment with business strategies; risk management; resource management; performance measurement ; value delivery. The output will be an approach for the successful and effective implementation of information security governance, especially in the oil industry.

Key words:
Information security, Information security governance, critical success factors, key performance indicator

1. PHD student, Information Technology Management, Islamic Azad University, Central Tehran Branch, Tehran, Iran (f63akhavan@gmail.com)
2. Assistant Professor, Industrial Management Dept, Information Technology Management, Islamic Azad University, Central Tehran Branch, Tehran, Iran (Corresponding Author) (saa.mousavi@iau.ac.ir)
3. Assistant Professor, Information Technology Management Dept, Tarbiat Modares University, Tehran, Iran(a.sarabadani@modares.ac.ir)

مقاله علمی ـ پژوهشی

◈

تاریخ دریافت ۱۴۰۱/۰۴/۲۷ **تاریخ پذیرش ۱۴۰۱ /۰۹/۲۶**

عوامل کلیدی موفقیت در پیاده‌سازی حاکمیت امنیت اطلاعات (مطالعهٔ موردی: شرکت نفت مناطق مرکزی ایران)

فاطمه اخوان[۱] ـ سید عبداله امین موسوی[۲] ـ ابوالقاسم سرآبادانی[۳]

چکیده

صنعت نفت به عنوان یکی از اصلی‌ترین و حیاتی‌ترین صنایع داخلی کشور، همواره با حملات سایبری و تهدیدات امنیتی مواجه بوده است. لذا ادغام امنیت اطلاعات در حاکمیت شرکتی ضروری و یک چالش حاکمیتی است. ادغام امنیت اطلاعات و حاکمیت شرکتی، حاکمیت امنیت اطلاعات نامیده می‌شود. در این پژوهش با استفاده از روش فراترکیب و مطالعهٔ منابع مرتبط با امنیت اطلاعات به شناسایی «عوامل کلیدی موفقیت» در پیاده‌سازی امنیت اطلاعات پرداختیم؛ زیرا قبل از هرگونه برنامه‌ریزی و سیاست‌گذاری در حوزهٔ حاکمیت امنیت اطلاعات توجه به این مقوله ضروری است. در ادامه این عوامل را بر اساس حوزه‌های تمرکز حاکمیت امنیت اطلاعات که شامل همسویی با استراتژی‌های کسب‌وکار؛ مدیریت ریسک؛ مدیریت منابع؛ اندازه‌گیری عملکرد؛ تحویل و ارائهٔ ارزش؛ طبقه‌بندی نمودیم. خروجی حاصل رویکردی برای پیاده‌سازی موفق و مؤثر حاکمیت امنیت اطلاعات به‌خصوص در مجموعهٔ صنعت نفت خواهد بود.

واژگان کلیدی: امنیت اطلاعات، حاکمیت امنیت اطلاعات، عوامل کلیدی موفقیت، شاخص‌های کلیدی مؤثر

---

۱. دانشجوی دکترای مدیریت فناوری اطلاعات، گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. f63akhavan@gmail.com

۲. استادیار گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده مسئول) saa.mousavi@iau.ac.ir

۳. استادیار گروه مدیریت فناوری اطلاعات، دانشگاه تربیت مدرس، تهران، ایران. a.sarabadani@modares.ac.ir

مقدمه

امروزه نقش پراهمیت اطلاعات و منابع اطلاعاتی در جوامع و حساسیت فرایندهای جمع‌آوری، ثبت و انتشار اطلاعات، دگرگونی بنیادینی را در ساختار مناسبات و ارتباطات جوامع ایجاد کرده است و با ایجاد نوآوری و فرصت‌های توسعه مزیت رقابتی، نقشی اساسی در تداوم موفقیت در کسب‌وکار دارد و همین امر، موجب ایجاد مخاطرات، تهدیدها و نگرانی‌های جدید مبتنی بر اطلاعات شده است. بدین ترتیب، حفظ محرمانه بودن، یکپارچگی و در دسترس بودن این منابع اطلاعاتی و حفظ امنیت برای سازمان‌ها ضروری است. (Carrow, 2014) (پیکری و بنازاده، ۱۳۹۷) صنعت نفت نیز به‌عنوان یکی از اصلی‌ترین و حیاتی‌ترین صنایع داخلی کشور، همواره مورد حملات سایبری از سوی هکرها قرارگرفته و با تهدیدات امنیتی مواجه بوده است. سازمان‌های امروز به‌شدت به دنبال تأمین امنیت اطلاعاتی از قبیل بانک اطلاعاتی مشتریان، اطلاعات مربوط به تولید محصول جدید و روش ساخت آن، اطلاعات مرتبط با نیروهای انسانی خود، اطلاعات و نتایج تحلیل‌های کسب‌وکار، اطلاعات سازمانی و غیره خود هستند تا در دست رقبا یا افراد غیرمجاز قرار نگیرد. هرچقدر سازمان‌ها بیشتر از سیستم‌های اطلاعاتی استفاده می‌کنند، اهمیت موضوع امنیت اطلاعات بیشتر و بیشتر می‌شود. (نورائی, ۱۳۹۱) درگذشته، امنیت اطلاعات صرفاً یک نگرانی فنی بود و کارکنان فنی مسئول امنیت اطلاعات در یک سازمان بودند. (آفتابی، ۱۳۹۷) این دیدگاه زمانی که به یک دیدگاه جامع و کل‌نگر و راهبرد کلی امنیت می‌رسد، شکست می‌خورد. (Diesch & et al, 2020) بر اساس مطالعات گروه سی‌جی‌آی (۲۰۱۶) شیوه‌های ضعیفی وجود دارد که امنیت اطلاعات را تضعیف و تهدید می‌کند؛ ازجمله: سیاست‌ها یا رویه‌های امنیتی موجود، سیاست‌های امنیتی منسوخ و یا نادیده گرفته شده، آگاهی ضعیف از اقدامات امنیتی در همه سطوح، شیوه‌های کنترل دسترسی ضعیف، عدم ممیزی و بررسی انطباق امنیت، عدم‌حمایت مدیریت ارشد و فقدان شخصیت مقتدر برای تصمیم‌گیری‌های مؤثر بر امنیت و یکپارچگی دارایی‌های زیرساختی و اطلاعاتی. (CGI, 2016) همچنین در تحقیقات الاحمد و محمد(۲۰۱۲) اشاره شده که در هر سازمانی، خطرات مربوط به امنیت اطلاعات باید شناسایی، ارزیابی، تجزیه‌وتحلیل، درمان و به‌درستی گزارش شود و

عدم توجه به این موضوع به علت عواملی مانند: عدم وجود تعهد و پشتیبانی مدیریت ارشد؛ عدم وجود سیاست‌های مناسب برای مدیریت ریسک امنیت اطلاعات؛ تجزیه و تفکیک تلاش‌ها در حوزه‌های حاکمیت، مدیریت ریسک و انطباق[1]، مدیریت ارزیابی‌های نادرست، مالکیت دارایی‌ها تعریف‌نشده، محدودیت‌های راه‌حل‌های خودکار موجود، وجود چندین چارچوب ارزیابی مخاطرات است. (Al-Ahmad & Mohammad, 2012)

حال مسئله این است که جهت پیاده‌سازی موفق امنیت اطلاعات هم‌راستا با کسب‌وکار سازمان چه عوامل و شاخص‌های کلیدی دخیل‌اند. لذا با توجه به نقش فزایندهٔ امنیت اطلاعات در ادارهٔ هر جامعه، سازمان‌ها و نهادهای دولتی و خصوصی ناگزیر به شناسایی شاخص‌های کلیدی امنیت اطلاعات و تأمین زیرساخت‌های لازم امنیتی برای بهبود وضعیت امنیت اطلاعات سازمان می‌باشند. شناسایی عوامل موفق و شاخص‌های کلیدی مؤثر[2] امنیت اطلاعات و آگاهی از وضعیت امنیت اطلاعات فعلی سازمان، منجر به اطمینان از اعمال توجه لازم به زمینه‌هایی است که موجب پیاده‌سازی موفق امنیت اطلاعات می‌شود. لذا قبل از هرگونه برنامه‌ریزی و سیاست‌گذاری در حوزهٔ امنیت اطلاعات توجه به این مقوله ضروری است.

فاکتورهای مهمی ازجمله مردم، فاکتورهای سازمانی، تکنولوژی، وظایف افراد و محیط کار، در برقراری امنیت پایدار تأثیرگذارند. (آفتابی،۱۳۹۷) از وظایف مدیران امنیت اطلاعات برای پیاده‌سازی موفق امنیت اطلاعات می‌توان به برنامه‌ریزی امنیتی، تعیین، توسعه و اجرای سیاست و الزامات امنیتی، مدیریت منابع انسانی، آگاهی و آموزش مستمر، همسویی کسب‌وکار و فناوری اطلاعات و مدیریت منابع انسانی، مدیریت زیرساخت‌های فناوری اطلاعات، مدیریت ریسک، انتخاب تکنولوژی امنیتی، توسعهٔ معماری مؤثر اطلاعات شرکت، ارزیابی تهدید، پیاده‌سازی اقدامات مقابله‌ای، نظارت بر عملکرد سیستم، نگهداری و حفاظت، رسیدگی و پاسخگویی و حصول اطمینان از انطباق و اجرای مؤثر و جامع چارچوب حاکمیت امنیت اطلاعات اشاره کرد. (ITGI, 2008) (Nazareth & Choi, 2015) (Maleh & et al,2017) (Diesch & et al, 2020) ضمن این‌که شناسایی عوامل موفق و شاخص‌های کلیدی مؤثر نیز برای بهبود وضعیت امنیت اطلاعات سازمان مهم و ضروری هستند. در پژوهشی تحت عنوان «عوامل موفقیت مدیریت امنیت سیستم‌های اطلاعاتی» را عواملی برای نشان دادن وضعیت عناصر دانستند که باید از

1. GRC: Governance, Risk Management, and Compliance.
2. CSFs: Critical Success Factors

شکست امنیت اطلاعات در زمینهٔ تجارت الکترونیکی جلوگیری کنند. (Norman & Yasin, 2013). در پژوهشی دیگر، عوامل حیاتی موفقیت را عواملی را توصیف می‌کنند که بر اجرای موفقیت‌آمیز یک سیستم مدیریت امنیت اطلاعات تأثیر می‌گذارند. (Tu & et al, 2014) و در پژوهشی دیگر محققان، عوامل حیاتی موفقیت را به‌عنوان حوزه‌های کلیدی در شرکت توصیف که نتایج نشان می‌دهد که با همسویی کسب‌وکار، پشتیبانی مدیریت ارشد و آگاهی سازمانی از خطرات و کنترل‌های امنیتی، می‌توان کنترل‌های امنیتی اطلاعات مؤثری را توسعه داد که منجر به مدیریت امنیت اطلاعات موفق و تضمین عملکرد می‌شود. (Tu & et al, 2018) در پژوهش دیش و همکاران (۲۰۲۰) توجه به عوامل موفقیت مدیریت[1] مانند اتخاذ تصمیمات مدیریتی و استراتژیک مناسب در زمینهٔ امنیت اطلاعات یک سازمان موردتوجه قرارگرفته است. برخی پژوهش‌ها فقط یک عامل را برجسته کردند، مانند عوامل سازمانی (ارنست چانگ و هو، ۲۰۰۶؛ هال و همکاران، ۲۰۱۱؛ کانکانهالی و همکاران، ۲۰۰۳؛ کریمر و همکاران، ۲۰۰۹؛ میجنهارت و همکاران، ۲۰۱۶؛ ناراین. سینگ و همکاران، ۲۰۱۴)، مسائل مربوط به انطباق با خط‌مشی (باس و همکاران، ۲۰۰۹؛ گوئل و چنگالور اسمیت، ۲۰۱۰؛ هون و الوف، ۲۰۰۲؛ ایفینیدو، ۲۰۱۲؛ جانستون و همکاران، ۲۰۱۶؛ لوری و مودی، ۲۰۱۵) یا عوامل انسانی (علوی و همکاران، ۲۰۱۶؛ آل هوگیل، ۲۰۱۵؛ آسندن، ۲۰۰۸؛ گونزالس و ساویکا، ۲۰۰۲؛ کریمر و همکاران، ۲۰۰۹). دلیل این تفکیک و تمرکز بر یک عامل، مدیریت جداگانه بر بحث امنیت در بخش‌های مختلف که شامل امنیت اطلاعات، مدیریت ریسک، تداوم کسب‌وکار، امنیت عملیاتی می‌شود. این‌ها نشان می‌دهد که مطالعات مختلفی در دسترس هستند که عوامل مختلف را با جزئیات زیاد موردبحث قرار می‌دهند، اما دیدگاهی جامع در مورد آن‌ها در برنمی‌گیرند. (Diesch & et al, 2020)

بر اساس نتایج حاصله از تحقیقات ارائه‌شده، امنیت اطلاعات در سازمان‌ها باید در حاکمیت شرکتی ادغام شود و به‌عنوان یک چالش حاکمیتی در نظر گرفته شود. (ITGI, 2006) ،(National Cyber Security Summit Task Force[2],2004)

1. MSFs: Management Success Factors

2. National Cyber Security Summit Task Force

کارگروه سران امنیت سایبری ملی، در دسامبر ۲۰۰۳ در آمریکا به منظور توسعه و ترویج یک چارچوب حاکمیتی منسجم شرکتی برای اجرای برنامه‌های امنیت اطلاعات موثر تشکیل شد؛ و هر ساله اقدام به برگزاری نشست ملی سایبری نوآورانه‌ترین رویداد فناوری امنیت سایبری کشورآمریکا می کند.

(Gashgari & et al, 2017) ادغام امنیت اطلاعات و حاکمیت شرکتی، حاکمیت امنیت اطلاعات نامیده می‌شود. حاکمیت امنیت اطلاعات، سیال، پویا و انعطاف‌پذیر است، زیرا محیط اجتماعی ـ فنی در حال تغییر است. (Williams & et al,2013) (Schinagl & Shahim,2019)

حاکمیت امنیت اطلاعات[1]، سامانه‌ای است که فعالیت‌های امنیت اطلاعات سازمان از طریق آن هدایت و کنترل می‌شود (سازمان ملی استاندارد ایران،۱۳۹۲). از دید گروه سی‌جی‌آی (۲۰۱۶) حاکمیت امنیتی چسبی است که تمام عناصر اصلی دفاع سایبری و مدیریت ریسک مؤثر را به هم متصل می‌کند و بدون آن خطرات ادامه دارد. علاوه بر این، رهبران ارشد از مواجهه با خطر سازمان خودآگاه نیستند که درنهایت آن‌ها مسئول خواهند بود. (CGI, 2016) ازآنجایی‌که حاکمیت امنیت اطلاعات از رهبری، ساختار سازمانی و فرایندها تشکیل‌شده است، رهبری باید مدیریت فعالانه داشته باشد و از این‌که فعالیت‌های امنیت اطلاعات در تمام سطوح سازمانی پشتیبانی، درک و اجرا می‌شود و با اهداف سازمانی همسو هستند، اطمینان حاصل نموده و آن را تضمین نماید. (National Cyber Security Summit Task Force,2004) (Rastogi & von Solms,2004) (ITGI,2006) (Love & et al, 2010) (Gashgari & et al, 2017)

جهت پیاده‌سازی و استقرار حاکمیت امنیت اطلاعات می‌توان از رایج‌ترین استانداردها و چارچوب‌های امنیت اطلاعات و فناوری اطلاعات بهره برد. یکی از رایج‌ترین استاندارد امنیت اطلاعات سری ISO/IEC270XX است. این استاندارد به‌طور گسترده پذیرفته شده و نقش مهمی ایفا می‌کند و می‌توان امنیت اطلاعات سازمانی را بر اساس آن تأیید کرد. (Haufe & al, 2016) (Diesch & et al, 2020) سری ISO/IEC270XX الزامات اساسی را برای پیاده‌سازی سیستم مدیریت امنیت اطلاعات تعریف می‌کند. همچنین، راهنمای کنترل، اجرا، اقدامات مدیریتی و رویکرد مدیریت ریسک مشخص‌شده است. علاوه بر استاندارد مدیریت امنیت اطلاعات، چارچوب‌ها یا بهترین شیوه‌ها مانند سری NIST SP800، استاندارد شیوه‌های مناسب از انجمن امنیت اطلاعات[2]، یا چارچوب کوبیتCOBIT و ITIL وجود دارد. این‌ها بهترین شیوه‌ها برای پیاده‌سازی امنیت اطلاعات هم‌راستا با کسب‌وکار سازمان ، تعریف و توسعهٔ کنترل‌ها و رسیدگی به مهم‌ترین مشکلات مربوط به امنیت اطلاعات هستند. (MIJNHARDT & et al, 2016)

1. ISG: information security governance
2. ISF: Information Security Forum

در این پژوهش تلاش شده است با توجه به اهمیت پیاده‌سازی امنیت اطلاعات هم‌راستا با کسب‌وکار سازمان و وجود چارچوب‌ها و رویکردهای مختلف پیشرو شرکت‌ها و سازمان‌ها با استفاده از روش فراترکیب و بررسی پژوهش‌های انجام‌شده در حوزهٔ امنیت اطلاعات، در ابتدا به بررسی و شناسایی شاخص‌های کلیدی امنیت اطلاعات پرداختیم و در ادامه به بررسی مفاهیم حاکمیت امنیت اطلاعات و حوزه‌های تمرکز آن پرداختیم. سپس با تجزیه‌وتحلیل و ترکیب نتایج مشابه، این اطلاعات دسته‌بندی‌شده و درنهایت با تلفیق با حوزه‌های تمرکز حاکمیت امنیت اطلاعات شامل: همسویی استراتژیک؛ مدیریت ریسک؛ مدیریت منابع ؛ اندازه‌گیری عملکرد؛ ارائه ارزش؛ رویکردی برای پیاده‌سازی موفق و مؤثر حاکمیت امنیت اطلاعات ارائه شده است که به کارشناسان و مدیران ارشد امنیت اطلاعات و فناوری اطلاعات به‌ویژه در صنعت نفت کمک کند تا عوامل تأثیرگذار جهت تصمیم‌گیری را در نظر بگیرد و سایر کارمندان نیز، نیازهای امنیتی را بهتر درک کنند و آگاهی خود را بهبود بخشند و این امر از سازمان‌ها و شرکت‌ها به‌خصوص شرکت‌های زیرمجموعه صنعت نفت، برای بقا و شکوفایی حمایت می‌کند.

روش پژوهش

پژوهش حاضر از نوع روش تحقیق فراترکیب یا متاسنتز و یک رویکرد کیفی مناسب برای مطالعات در حوزهٔ مدیریت با فراهم کردن یک نگرش نظام‌مند برای محققان از طریق ترکیب تحقیقات کیفی مختلف به کشف موضوعات و استعاره‌های جدید و اساسی می‌پردازد و با این روش دانش جاری را ارتقاء داده و یک دید جامع و گسترده نسبت به مسائل به وجود می‌آورد. (Noblit & Hare, 1988) از دیدگاه زیمبر فراترکیب صرفاً بررسی ادبی متشکل از یک حوزهٔ خاص و یا تجزیه‌وتحلیل ثانویه داده‌های اولیه از یک گروه از مطالعات تحقیقاتی نیست، بلکه تفسیری از یافته‌های مطالعات انتخاب شده است؛ به‌عبارت‌دیگر، محققانی که از فراترکیب استفاده می‌کنند، نه‌تنها سنتز یافته‌های یک مجموعه با دقت انتخاب شده از مطالعات را انجام می‌دهند، بلکه به‌طورجدی به تجزیه‌وتحلیل و تفسیر پیچیده و عمیق این داده‌ها می‌پردازند. (Zimmer, 2006) در فراترکیب اگرچه مطالعات زیادی مرور می‌شوند، اما هدف از این کار تنها انتقاد به تحقیقات انجام‌شده نیست، بلکه هدف آن است که افق دید افراد گسترش‌یافته و دانش جدیدی ایجاد شود. (Sandelowski, 2007) درک این موضوع که این رویکرد صرفاً یک

بررسی جامع یا خلاصه‌ای از ادبیات موجود نیست، بلکه یک سنتز و تحلیل بسیار پیچیده از تحقیقات کیفی است مهم است. (Erwin & et al, 2011) انجام فراترکیب مستلزم این است که محقق یک بازنگری دقیق و عمیق را در خصوص موضوع مدنظر انجام داده و یافته‌های تحقیقات کیفی مرتبط را با یکدیگر ترکیب کند. به این منظور از روش هفت مرحله‌ای سندلوسکی و باروسو شامل مراحل: ۱. تنظیم سؤال پژوهش، ۲. مرور نظام‌مند پیشینه، ۳. جستجو و انتخاب مقالات مناسب، ۴. استخراج اطلاعات مقالات، ۵. تجزیه‌وتحلیل و ترکیب یافته‌های کیفی، ۶. کنترل کیفیت و ۷. ارائه یافته‌ها استفاده می‌شود. (Sandelowski, 2007) لذا با توجه به اهمیت این موضوع و وجود چارچوب‌ها و رویکردهای مختلف پیشرو شرکت‌ها و سازمان‌ها، در این پژوهش با استفاده از روش فراترکیب و بررسی پژوهش‌های انجام‌شده در حوزهٔ امنیت اطلاعات، در ابتدا به بررسی مفاهیم حاکمیت امنیت اطلاعات پرداختیم و در ادامه در پژوهش‌ها و مقالات مرتبط با موضوع طی سال‌های اخیر (جستجوی اینترنتی شامل کتب، مقـالات، گزارش‌ها و مطالعات مـوردی) بررسی شده‌اند که منجر به مشخص شدن کلیدواژه‌های اصلی و ادامه مسیر از میان ۱۳۰ پژوهش شد. در ادامه با بررسی تفسیری مقالات و غربالگری، ۱۰۰ مورد از پژوهش به موضوع ارتباط بیشتری داشتند، تفکیک و این موارد نیز به دو حوزهٔ فناوری اطلاعات (۳۵ مورد) و امنیت اطلاعات (۶۵ مورد) تقسیم شده و جهت سنجش اعتبار منابع پژوهش با توجه به ماهیت تحقیق که کیفی است و برخلاف پژوهش‌های کمّی هیچ آزمون استانداری برای روایی وجود ندارد و اغلب ماهیت پژوهش توسط پژوهشگر تعیین و تعدیل می‌شود و ماهیت مفهوم روایی در پژوهش‌های کیفی به بازنمایی مشارکت‌کنندگان، اهداف پژوهش و مناسب بودن فرایندها ارتباط دارد. (فقیهی و علیزاده،۱۳۸۴) در این پژوهش منابع با استفاده از ابزار ارزیابی مهارت‌های کیفیت CASP[1] بررسی و با استفاده از چک‌لیست مرتبط با ارزیابی پژوهش‌های کیفی که ۱۰ سؤال ارائه می‌کند که نتایج حاصل از آن به محقق کمک می‌کند تا دقت، اعتبار و اهمیت مطالعه‌ها کیفی تحقیق را مشخص کند. این سؤالات بر موارد زیر تمرکز دارد: ۱. اهداف تحقیق، ۲. روش‌شناسی، ۳. طرح تحقیق، ۴. استراتژی و روش نمونه‌برداری و انتخاب شرکت‌کنندگان، ۵. جمع‌آوری داده‌ها، ۶. جهت‌گیری محقق (رابطه بین محقق و شرکت‌کنندگان)، ۷. ملاحظات اخلاقی، ۸. دقت در تجزیه‌وتحلیل داده‌ها، ۹. بیان واضح

1. CASP: Critical Appraisal Skills Program

برنامه و ابزاری جهت ارزیابی مطالعات کیفی ارائه شده توسط CASPUK

و روشن یافته‌ها و ۱۰. ارزش پژوهش؛ که پاسخ به دو سؤال اول کمک شایانی به پژوهشگر جهت ادامه روند پاسخگویی و مفید بودن منبع جهت ارزیابی ارائه می‌کند. پاسخ به هر سؤال به‌صورت کیفی و سه پاسخ «بله»، «نه» یا «نمی‌توانم بگویم» است؛ که با معادل قرار دادن یک امتیاز کمّی به هر پاسخ و جمع امتیازها، میزان اثر پژوهش در این مرحله مشخص می‌شود و مواردی که زیر امتیاز میانگین مجموع امتیازات باشد، اثر بسیار کمتری دارند و غربال و حذف می‌شوند. (CASPUK,2022) در گام بعد شناسایی شاخص‌های کلیدی و عوامل مؤثر در امنیت اطلاعات، محور تحقیقات قرارگرفته است. سپس با تجزیه‌وتحلیل و ترکیب نتایج مشابه این اطلاعات دسته‌بندی‌شده و در ادامه حوزهٔ تمرکز حاکمیت امنیت اطلاعات موردتوجه قرارگرفت. درنهایت با تلفیق شاخص‌ها و عوامل کلیدی موفقیت در امنیت اطلاعات و حوزه‌های تمرکز حاکمیت امنیت اطلاعات، رویکردی برای پیاده‌سازی موفق و مؤثر حاکمیت امنیت اطلاعات ارائه‌شده است که به هیئت حاکمه و مدیران ارشد فناوری اطلاعات و امنیت اطلاعات در درک درست و بر «چگونگی» و «آنچه» باید انجام شود، جهت دستیابی به وضعیت قابل‌قبول امنیت اطلاعات کمک می‌کند و تأثیر مستقیم بر تصمیم‌گیری‌ها، سیاست‌گذاری، تعیین اهداف استراتژیک سازمانی و اطمینان از دستیابی آن‌ها، مدیریت منابع و بهینه‌سازی سرمایه‌گذاری‌ها و موفقیت بلندمدت سازمان‌ها و شرکت‌ها به‌خصوص در حوزهٔ صنعت نفت و شرکت‌ها می‌گذارد.

یافته‌ها

حوزه‌های تمرکز حاکمیت امنیت اطلاعات

بر اساس پژوهش‌های و راهنماهای پیشین مانند تحقیقات مؤسسهٔ حاکمیت فناوری اطلاعات[1] (۲۰۰۸)، لوفن (۲۰۱۹) و نیکو (۲۰۱۸)، برای دستیابی به پیشرفت‌های قابل‌توجه، امنیت اطلاعات باید بخشی جدایی‌ناپذیر از حاکمیت سازمانی باشد و در استراتژی، مفهوم، طراحی، اجرا و عملیات ادغام شود. امنیت اطلاعات باید تقریباً در تمام استراتژی‌های مدیریت در نظر گرفته شود و به‌عنوان عاملی حیاتی در موفقیت شناخته شود. حاکمیت مؤثر امنیت اطلاعات مستلزم تعهد مدیریت ارشد و یک فرهنگ

1. ITGI: IT Governance Institute

موسسه حاکمیت فناوری اطلاعات، توسط انجمن غیرانتفاعی ISACA در سال ۱۹۹۸ تأسیس شد. که راهنمایی‌های لازم برای جامعه تجاری جهانی در مورد مسائل مربوط به حاکمیت دارایی های فناوری اطلاعات ارائه می‌کند.

کلی برای امنیت اطلاعات در سطوح اجرایی و عملیاتی است. حاکمیت امنیت اطلاعات شامل عناصر موردنیاز برای ایجاد اطمینان مدیریت ارشد مبنی بر این‌که جهت و هدف آن در وضعیت امنیتی سازمان با استفاده از یک رویکرد ساختاریافته برای اجرای یک برنامه امنیت اطلاعات منعکس می‌شود، است. هنگامی‌که این عناصر در جای خود قرار گرفتند، مدیریت ارشد می‌تواند اطمینان داشته باشد که امنیت اطلاعات کافی و مؤثر خواهد بود. بدیهی است که هیچ مقیاس و هدف جهانی برای امنیت اطلاعات یا حاکمیت امنیت اطلاعات وجود ندارد. ازآنجایی‌که سنجش حاکمیت، به‌طورکلی و حاکمیت امنیت اطلاعات به‌طور خاص، دشوار است که با مجموعه‌ای از معیارهای عینی اندازه‌گیری شوند، تمایل به استفاده از معیارهایی وجود دارد که بدون توجه به ارتباط ثابت‌شده در دسترس هستند. برای سازمانی که هدف یا اهداف امنیت اطلاعات را مشخص کرده است، معیارها را می‌توان به هر معیاری از نتایج برنامه امنیت اطلاعات که به سمت اهداف تعریف‌شده پیش می‌رود کاهش داد. با این رویکرد، راهنمایی مفید برای توسعهٔ معیارهای خاص سازمان از سوی سازمان‌هایی مانند اساکا[1]، سِرت[2]، مؤسسهٔ حاکمیت فناوری اطلاعات، انجمن امنیت سیستم‌های اطلاعات[3]، مؤسسهٔ بین‌المللی فناوری و استانداردها[4] امکان‌پذیر است. هدف امنیت اطلاعات توسعه، اجرا و مدیریت یک برنامه امنیت اطلاعات است که به پنج نتیجه اساسی مشخص‌شده در حاکمیت امنیت اطلاعات دست یابد:

ـ همسویی استراتژیک امنیت اطلاعات با استراتژی کسب‌وکار برای حمایت از اهداف سازمانی

ـ مدیریت ریسک مؤثر با اجرای اقدامات مناسب برای مدیریت و کاهش خطرات و کاهش اثرات بالقوه بر منابع اطلاعاتی تا سطح قابل‌قبول

ـ مدیریت منابع با استفاده از دانش و زیرساخت امنیت اطلاعات به‌طور کارآمد و مؤثر

ـ اندازه‌گیری عملکرد با اندازه‌گیری، نظارت و گزارش معیارهای حاکمیت امنیت اطلاعات برای اطمینان از دستیابی به اهداف سازمانی

ـ ایجاد ارزش با بهینه‌سازی سرمایه‌گذاری‌های امنیت اطلاعات در حمایت از اهداف سازمانی (ITGI, 2008) (Loeffen, 2019) (Nicho, 2018)

1. ISACA: Information Systems Audit and Control Association
2. CERT: Computer emergency response team
3. ISSA: Information Systems Security Association
4. NIST: National Institute of Standards and Technology

شاخص‌ها و عوامل کلیدی موفقیت در پیاده‌سازی حاکمیت امنیت اطلاعات

بزرگ‌ترین مسئله در دنیای رقابتی برای سازمان‌ها ایجاد و تقویت مزیت‌های رقابتی، کاهش هزینه‌ها و ارتقای بهره‌وری عملیاتی به‌عنوان عوامل کلیدی موفقیت سازمان می‌باشند (اصغرپور،۱۳۷۷) و اطلاعات یک منبع کلیدی و استراتژیک و سرمایه در جهت رشد و موفقیت برای سازمان‌ها محسوب می‌شود که به‌وسیله آن می‌توان ارزش‌افزوده محصولات و خدمات را افزایش داد. هم‌زمان با گسترش استفاده سازمان‌ها از منابع اطلاعاتی گوناگون، نیاز به حفظ امنیت این منابع نیز بیشتر می‌شود. وضعیت امنیت اطلاعات یک سازمان و شناسایی شاخص‌های کلیدی امنیتی برای بهبود وضعیت امنیت اطلاعات سازمان مهم هستند و سازمان برای رقابت موفقیت‌آمیز و مدیریت زمان و هزینه‌های خود نیازمند تمرکز و توجه به آن‌هاست. با توجه به بررسی‌های به‌عمل‌آمده در پژوهش‌های پیشین، شاخص‌های کلیدی پیاده‌سازی موفق امنیت اطلاعات با تجزیه‌وتحلیل جامع ادبیات دانشگاهی و عمل‌گرا مربوط به اجرای حاکمیت امنیت اطلاعات و سایر رشته‌های مرتبط مانند امنیت اطلاعات، امنیت سازمانی به‌دست‌آمده است که در جدول ۱ ذکرشده است.

جدول ۱. شاخص‌ها و عوامل کلیدی موفقیت امنیت اطلاعات شناسایی‌شده

ردیف	شاخص‌های کلیدی مؤثر امنیت اطلاعات	منبع
۱	امنیت اطلاعات را با فعالیت‌های کسب‌وکار و چرخه عمر سیستم‌ها و پروژه‌ها یکپارچه کنید	(Bowen & et al, 2006); (ITGI,2006); (ITGI,2008); (Allen, 2013); (Bobbert & Mulder, 2015)(Gashgari & et al, 2017); (Nicho, 2018); (ISO, 2022) (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری، ۱۳۹۴)؛ (عیسی‌زاده،۱۳۹۴)
۲	همسویی استراتژیک با فعالیت‌های سازمان در حال انجام	(Rastogi & von Solms, 2004); (ITGI,2006); (ITGI,2008); (Bobbert & Mulder, 2015); (Nazareth & Choi, 2015): (CGI,2016); (Maleh & et al,2017); (Gashgari & et al, 2017); (Nicho, 2018); (ISACA, 2018); (ISO, 2022); (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری، ۱۳۹۴)؛ (اخوان و رادفر، ۱۳۹۹)
۳	اراده، تعهد، مشارکت و پشتیبانی مدیریت ارشد قابل‌مشاهده	(Williams, 2001); (de Oliveira Alves G. A., 2006); (ITGI,2006); (Bowen & et al ,2006); (Westby & Allen,2007); (ITGI,2008); (Allen, 2013);(Gashgari & et al, 2017); (Nicho, 2018); (ISACA, 2018) (ISO, 2022) (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری، ۱۳۹۴)؛ (عیسی‌زاده،۱۳۹۴)؛ (اخوان و رادفر، ۱۳۹۹)

۴	مدیریت پروژهٔ قوی	(ITGI,2008); (Nazareth & Choi, 2015): (Maleh & et al,2017); (Gashgari & et al, 2017); (Nicho, 2018); (ISO, 2022) (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری، ۱۳۹۴)؛ (رضایی و همکاران، ۱۳۹۷)
۵	مدیریت تغییر	(CGI, 2016); (Gashgari & et al, 2017); (ISO, 2022) (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری، ۱۳۹۴)؛ (رضایی و همکاران، ۱۳۹۷)؛
۶	نظام پذیرش سیستم و ایجاد یک محیط امنیتی مثبت	(Gashgari & et al, 2017); (Nicho, 2018); (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری، ۱۳۹۴)(اخوان و رادفر، ۱۳۹۹)
۷	اطمینان حاصل کنید که سیاست‌ها و شیوه‌های امنیت اطلاعات با قوانین و مقررات و الزامات مربوطه مطابقت دارند	(Williams, 2001);(Bowen & et al, 2006);(ITGI,2006); (ITGI,2008); (CGI, 2016); (Gashgari & et al, 2017); (Nicho, 2018); (ISO, 2022) (عیسی‌زاده،۱۳۹۴)؛ (اخوان و رادفر، ۱۳۹۹)
۸	تعیین دامنه، نقشهٔ راه، قلمرو و اهداف امنیتی از اجرا سیستم	(ITGI,2008); (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری، ۱۳۹۴)؛ (عیسی‌زاده،۱۳۹۴)؛ (رضایی وهمکاران، ۱۳۹۷)؛ (اخوان و رادفر، ۱۳۹۹)
۹	تحلیل شکاف مناسب قبل از پیاده‌سازی استاندارد	(ISO, 2022) (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری، ۱۳۹۴)؛
۱۰	الگوبرداری مناسب	(ITGI,2008); (ISO, 2022) (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری، ۱۳۹۴)؛ (عیسی‌زاده،۱۳۹۴)
۱۱	انتخاب و به‌کارگیری مشاور توانمند در پیاده‌سازی	ITGI,2008); (Nicho, 2018) (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری، ۱۳۹۴)
۱۲	سیاست‌های امنیتی متناسب با دارایی‌ها	(ITGI,2008); (Nazareth & Choi, 2015); (Maleh & et al,2017); (Nicho, 2018); (ISO, 2022) (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری، ۱۳۹۴)
۱۳	به‌کارگیری تجربیات قبلی سازمان در خصوص پیاده‌سازی سایر استانداردهای مدیریتی معتبر	(Nicho, 2018) (خیری، ۱۳۹۴)؛ (عیسی زاده،۱۳۹۴)
۱۴	شناسایی دارایی و ریسک موجود، تحلیل، ارزیابی دقیق و به‌کارگیری کنترل مناسب	(ITGI,2008); (Nazareth & Choi, 2015); (Maleh & et al, 2017); (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری،۱۳۹۴)؛ (اخوان و رادفر، ۱۳۹۹)
۱۵	تدوین خط‌مشی و دستورالعمل‌ها بر اساس واقعیت سازمان	(ITGI,2008); (Nicho, 2018); (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری،۱۳۹۴)؛

۱۶	مشخص کردن جهت تصمیم‌های سرمایه‌گذاری	(ITGI,2008); (CGI, 2016); (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری،۱۳۹۴)؛(عیسی زاده،۱۳۹۴)
۱۷	سرمایه‌گذاری و تعهد منابع کافی در امنیت اطلاعات	(ITGI,2006); (de Oliveira Alves G. A., 2006); (Westby & Allen, 2007)(ITGI,2008); (Allen, 2013); (Nazareth & Choi,2015) ; (CGI, 2016); (Maleh & et al, 2017); (Gashgari & et al, 2017); (Nicho, 2018); (ISACA, 2018); (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری،۱۳۹۴)؛ (عیسی زاده،۱۳۹۴)
۱۸	آگاهی و آموزش مؤثر و مستمر امنیت اطلاعات	(Williams, 2001); (Bowen & et al, 2006);(ITGI,2006); (Westby & Allen, 2007);(ITGI,2008); (Allen, 2013); (Bobbert & Mulder, 2015); (Nazareth & Choi, 2015); (CGI, 2016); (Maleh & et al, 2017); (Gashgari & et al, 2017); (Nicho, 2018); (ISACA, 2018) (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری،۱۳۹۴)؛ (عیسی زاده،۱۳۹۴)؛ (رضایی و همکاران، ۱۳۹۷)
۱۹	ایجاد فرهنگ امنیتی در سازمان و توسعهٔ کار تیمی	(ITGI,2008); (Gashgari & et al, 2017); (Nicho, 2018);(ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری،۱۳۹۴)؛ (عیسی زاده,۱۳۹۴)؛ (رضایی و همکاران، ۱۳۹۷)؛ (اخوان و رادفر، ۱۳۹۹)
۲۰	تداوم کسب‌وکار / طرح بازیابی فاجعه	(Williams, 2001);(National Cyber Security Summit Task Force,2004) (ITGI,2006); (ITGI,2008); (Allen, 2013); (Gashgari & et al, 2017); (Nicho, 2018); (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری،۱۳۹۴)؛ (رضایی و همکاران، ۱۳۹۷)؛ (اخوان و رادفر، ۱۳۹۹)
۲۱	مشارکت و همکاری کارکنان	(ITGI,2008); (Nicho, 2018); (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری،۱۳۹۴)؛ (اخوان و رادفر، ۱۳۹۹)
۲۲	تعیین و آگاهی از سطح ریسک قابل‌قبول	(Williams, 2001) ; (Love & et al, 2010); (Allen, 2013); (Bobbert & Mulder, 2015); (CGI, 2016);(Gashgari & et al, 2017);
۲۳	کاربردهای حیاتی و سیستم‌های اطلاعاتی را شناسایی کنید	(National Cyber Security Summit Task Force,2004) (ITGI,2006); (ITGI,2008); (Gashgari & et al, 2017); (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری،۱۳۹۴)
۲۴	حفاظت از دارایی‌های حساس	(ITGI,2008); (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛
۲۵	اطمینان از ارزیابی منظم ریسک و تهدید	(National Cyber Security Summit Task Force,2004) (ITGI,2006); (Westby & Allen, 2007);(ITGI,2008); (Love & et al, 2010); (Bobbert & Mulder, 2015); (Nazareth & Choi, 2015); (CGI, 2016); (Maleh & et al,2017 (Gashgari & et al, 2017); (Nicho,

		2018); (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری،۱۳۹۴)؛ (عیسی زاده,۱۳۹۴)؛ (رضایی و همکاران، ۱۳۹۷)؛ (اخوان و رادفر، ۱۳۹۹)
۲۶	اطمینان از ارائه گزارش به‌موقع و شفاف عملکرد و مسائل امنیت اطلاعات	(National Cyber Security Summit Task Force,2004); (ITGI,2006); (Westby & Allen, 2007); (ITGI,2008); (Bobbert & Mulder, 2015); (Gashgari & et al, 2017; (Nicho, 2018); (ISO, 2022) (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری،۱۳۹۴)
۲۷	بررسی مستمر عملکرد امنیت اطلاعات	(National Cyber Security Summit Task Force,2004) (ITGI,2006); (Bowen & et al,2006); (Westby & Allen,2007); (ITGI,2008); (Nazareth & Choi,2015); (CGI, 2016);(Maleh & et al, 2017); (Gashgari & et al, 2017);(Nicho, 2018); (ISO, 2022) (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری،۱۳۹۴)؛ (اخوان و رادفر، ۱۳۹۹)
۲۸	مدیریت و پایش پروژه منطبق بر استاندارد مدیریت پروژه	(CGI, 2016)؛ (خیری، ۱۳۹۴)
۲۹	ممیزی مستمر داخلی و تضمین انطباق با الزامات داخلی و خارجی و ارائه گزارش به مدیریت ارشد	(ITGI,2008);(Nazareth & Choi, 2015); (CGI, 2016)(Maleh & et al, 2017); (ISO, 2022) (سازمان ملی استاندارد ایران،۱۳۹۲)؛ (خیری،۱۳۹۴)؛(اخوان و رادفر، ۱۳۹۹)
۳۰	تعیین دقیق شاخص‌های اثربخشی سیستم و اندازه‌گیری و تحلیل مستمر آن‌ها	(Bobbert & Mulder, 2015); (Gashgari & et al, 2017); (Nicho, 2018) (خیری، ۱۳۹۴)؛ (رضایی و همکاران، ۱۳۹۷)
۳۱	بهبود امنیت اطلاعات در ارتباط با نتایج کسب وکاربه صورت مستمر	(National Cyber Security Summit Task Force,2004)(ITGI,2006); (ITGI,2008); (Gashgari & et al, 2017); (Nicho, 2018); (ISO, 2022) (سازمان ملی استاندارد ایران، ۱۳۹۲)؛ (خیری،۱۳۹۴)؛ (اخوان و رادفر، ۱۳۹۹)

همان‌طور که پیش‌ازاین اشاره شد برای این‌که حاکمیت امنیت اطلاعات به‌درستی اجرا شود باید پنج نتیجه را ارائه دهد: همسویی استراتژیک؛ مدیریت ریسک؛ مدیریت منابع؛ اندازه‌گیری عملکرد؛ تحویل و ارائه ارزش؛ بنابراین، رهبران سازمانی باید در این زمینه‌های ضروری با موفقیت عمل کنند. شاخص‌های کلیدی مؤثر امنیت اطلاعات شناسایی‌شده در مرحلهٔ قبل که در جدول ۱ ذکر شده است، در سراسر این حوزه‌های ضروری حاکمیت امنیت اطلاعات که جزء چرخه حیات حاکمیت فناوری اطلاعات نیز هستند، مستقر می‌شوند و بر اساس تلفیق این شاخص‌ها و عوامل با حوزه‌های تمرکز حاکمیت امنیت اطلاعات، رویکرد پیشنهادی در جدول ۲ برای ارائه

راهنمایی روشن در مورد اجرای مهم‌ترین شیوه‌های حکمرانی در میان حوزه‌های ضروری حاکمیت امنیت ایجادشده است. نتایج حاصل نشان می‌دهد که شاخص‌های کلیدی و عوامل مؤثر در موفقیت بر روی حکمرانی مؤثر امنیت اطلاعات تأثیر می‌گذارد، بنابراین به هدف تحقیق دست می‌یابد.

جدول ۲. رویکرد پیشنهادی و راهنمایی برای شاخص‌ها و عوامل کلیدی موفقیت در پیاده‌سازی حاکمیت امنیت اطلاعات

منطقه (محدوده) حاکمیت امنیت اطلاعات	راهنمایی	شاخص‌ها و عوامل کلیدی موفقیت	هدف کلیدی
همسویی استراتژیک	امنیت اطلاعات را به عنوان یک موضوع گسترده سازمان در نظر بگیرید	برنامه امنیت اطلاعات به وضوح فعالیت‌های کسب و کار خاصی را امکان پذیر می کند.	هدف کلیدی امنیت اطلاعات کاهش اثرات نامطلوب بر سازمان به سطح قابل قبول و تضمین حفظ کسب و کار است.
		سازمان امنیت اطلاعات و نقش‌ها و مسئولیت های امنیت اطلاعات به الزامات کسب و کار تعریف شده پاسخگو است.	
		اهداف سازمانی و امنیت اطلاعات توسط همه موارد درگیر در امنیت اطلاعات و فعالیت های تضمینی مرتبط تعریف شده و به وضوح درک می شود.	
	حرفه‌ای و اخلاقی عمل کنید	امنیت اطلاعات و خط مشی کنترل اطلاعات را با برنامه‌های استراتژیک کلی همسو و با فعالیت‌های کسب‌وکار ادغام نموده و این برنامه و نقشه راه توسط مدیریت اجرایی تایید شده باشد.	مشارکت و رهبری قابل مشاهده
	پیروی و مطابقت با الزامات داخلی و خارجی امنیت اطلاعات	یک کمیته راهبری امنیت اطلاعات متشکل از مدیران کلیدی با منشوری برای اطمینان از همسویی مداوم فعالیت‌های امنیت اطلاعات و استراتژی کسب و کار وجود دارد.	
مدیریت ریسک	رویکرد مبتنی بر ریسک به طور مستمر و نظام مند،	ریسک‌پذیری یا تحمل ریسک سازمانی با عبارات مرتبط با سازمان تعریف می‌شود.	یک استراتژی و برنامه کلی امنیت اطلاعات برای دستیابی به سطوح

	اتخاذ کنید	ارزیابی کامل و منظم دارایی و واگذاری مالکیت و شناسایی ریسک و تهدیدات	قابل قبول ریسک و کاهش اثرات نامطلوب بر سازمان به سطح قابل قبول و تضمین حفظ کسب و کار
		شناسایی و تعریف اهداف کاهش خطرات قابل توجه	
		وجود فرآیندهایی برای مدیریت یا کاهش اثرات نامطلوب	
		روند ارزیابی ریسک دوره‌ای نشان‌دهنده پیشرفت در جهت اهداف تعریف شده است.	
	حفاظت از اطلاعات طبقه‌بندی شده	شناسایی کاربردهای حیاتی و سیستم های اطلاعاتی	حفاظت از دارایی های حساس
	روی برنامه‌های کاربردی کسب‌وکار مهم تمرکز کنید	یک طرح تداوم کسب و کار[1] آزمایش شده /طرح بازیابی فاجعه[2] وجود دارد.	طرح تداوم کسب و کار / طرح بازیابی فاجعه
		اهداف زمان بازیابی[3] برای همه سیستم های حیاتی توسعه یافته است.	
مدیریت موثر منابع	فرهنگ مثبت امنیت اطلاعات را پرورش دهید	آگاهی و آموزش مؤثر امنیت اطلاعات	توصیف فرآیندهای برنامه‌ریزی، تخصیص و کنترل منابع امنیت اطلاعات، از جمله افراد، فرآیندها و فناوری‌ها برای بهبود کارایی و اثربخشی راه‌حل‌های کسب و کار
	جهت تصمیمات سرمایه‌گذاری را تعیین کنید	سرمایه گذاری و تعهد منابع کافی امنیت اطلاعات	
		جذب و انتشار دانش مؤثر	
		استفاده از فرآیندهای استاندارد	
		تعریف نقش‌ها و مسئولیت‌ها برای عملکردهای امنیت اطلاعات به‌طور شفاف	
		گنجانده شدن عملکردهای امنیت اطلاعات در هر طرح پروژه	
		دارایی های اطلاعاتی و تهدیدات مرتبط تحت پوشش منابع امنیتی	
سنجش و اندازه‌گیری عملکرد	ارائه اطلاعات به موقع و دقیق در	زمان لازم برای شناسایی و گزارش حوادث مربوط به امنیت اطلاعات	حصول اطمینان از ارائه گزارش به موقع و شفاف

1. BCP: Business Continuity Plan
2. DRP: Disaster Recovery Plan
3. RTO: Recovery Time Objective

	مورد عملکرد امنیت اطلاعات	تعداد و فراوانی حوادث گزارش نشده بعدی کشف نشده	عملکرد و مسائل امنیت اطلاعات
		مکان مناسب در ساختار سازمانی، سطح اختیارات و تعداد پرسنل برای عملکرد امنیت اطلاعات وجود داشته باشد.	
	بررسی عملکرد امنیت اطلاعات در رابطه با نتایج کسب و کار	معیارها با سازمان‌های قابل مقایسه برای هزینه و اثربخشی	سنجش عملکرد امنیت اطلاعات با استفاده از یک فرآیند تایید برای اندازه‌گیری آگاهی، درک و انطباق با خط‌مشی‌ها، ثبت و تجزیه و تحلیل
		توانایی تعیین اثربخشی و کارایی کنترل‌ها	
		نشانه واضحی مبنی بر تحقق اهداف امنیت اطلاعات	
	ارتقاء بهبود مستمر در امنیت اطلاعات	عدم وجود رویدادهای غیرمنتظره امنیت اطلاعات	یک چارچوب توسعه خط مشی به‌طور مداوم اعمال می‌شود که فرمول‌بندی، گسترش، درک و انطباق را راهنمایی می‌کند. و بررسی مستمر استراتژی و عملکرد امنیت اطلاعات توسط شخص ثالث برای افزایش عینیت
		آگاهی از تهدیدات قریب‌الوقوع	
		ابزار موثر برای تعیین آسیب‌پذیری های سازمانی	
		روش‌های ردیابی خطرات در حال تحول	
ارائه ارزش	ارائه کیفیت و ارزش به ذینفعان	طراحی فعالیت‌های امنیت اطلاعات برای دستیابی به اهداف استراتژیک خاص	سطوح سرمایه‌گذاری بهینه متناسب با اهداف استراتژیک برای امنیت اطلاعات و وضعیت ریسک قابل قبول با کمترین هزینه
		ارزیابی درجه ریسک و تأثیر بالقوه منابع امنیت اطلاعات	
		کنترل‌ها به‌خوبی بر اساس اهداف کنترلی تعریف شده، طراحی شده‌اند و به‌طور کامل مورد استفاده قرار می‌گیرند . و تاثیر قابل قبول، کافی و مناسب است.	
		کنترل اثربخشی با استفاده از آزمایش دوره‌ای	
		ارزیابی مجدد اثربخشی و انطباق و هزینه‌های سیاست‌هایی کنترل دوره‌ای	

نتیجه‌گیری

یک برنامه امنیت اطلاعات سازمانی مؤثر شامل: استفاده از استانداردها و چارچوب‌های و روش‌های بین‌المللی امنیتی که موجب جذب اعتماد ذینفعان می‌شود، تجزیه‌وتحلیل آمار و گزارش و معیارهای عملکرد اطلاعات، ارائه راه‌حل وقایع امنیت اطلاعات و حسابرسی است و امنیت اطلاعات باید در بالاترین سطوح سازمان ازجمله هیئت‌مدیره، مدیران اجرایی و مدیریت موردتوجه قرار گیرد و این مسئله از طریق ادغام امنیت اطلاعات با حاکمیت شرکتی میسر می‌شود. حاصل این ادغام حاکمیت امنیت اطلاعات است. برای اجرای حاکمیت مؤثر امنیت اطلاعات، ضروری است که شاخص‌های کلیدی موفقیت در پیاده‌سازی حاکمیت امنیت اطلاعات که بر موفقیت بلندمدت سازمان‌ها تأثیر می‌گذارد، شناسایی شوند. شاخص‌های کلیدی امنیتی برای بهبود وضعیت امنیت اطلاعات سازمان مهم هستند. در بسیاری از پژوهش‌های پیشین به عوامل و شاخص کلیدی موفق امنیت اطلاعات در حوزهٔ مدیریت امنیت اطلاعات و یا صرفاً به چند و یا یک عامل تمرکز شده است؛ اما رویکرد پیشنهادی در این مقاله به شناسایی شاخص‌های کلیدی موفقیت امنیت اطلاعات و طبقه‌بندی و تلفیق آن‌ها با حوزه‌های تمرکز حاکمیت امنیت اطلاعات شامل: همسویی استراتژیک؛ مدیریت ریسک؛ مدیریت منابع؛ اندازه‌گیری عملکرد؛ ارائه ارزش؛ معطوف شده است که می‌تواند به کارشناسان و مدیران ارشد امنیت اطلاعات و فناوری اطلاعات به‌ویژه در صنعت نفت کمک کند تا دیدگاهی جامعی در مورد وابستگی‌های متقابل بین مفاهیم مرتبط پیدا کنند و با آگاهی از عوامل تأثیرگذار در اتخاذ تصمیمات و توجیه حجم سرمایه‌گذاری انجام‌شده و مدیریت زمان در ایجاد و توسعهٔ حاکمیت امنیت اطلاعات میسر شود و سایر کارمندان نیز نیازهای امنیتی و تصمیمات خاص در این زمینه را بهتر درک کنند و درنتیجه آگاهی خود را بهبود بخشند. که همهٔ این عوامل تأثیر مستقیم بر موفقیت بلندمدت سازمان‌ها و شرکت‌ها دارد.

منابع

اخوان، ف؛ رادفر، ر (۱۳۹۹)، ارائهٔ مدلی برای پایش بلوغ امنیت اطلاعات. *فصلنامهٔ رشد فناوری* ،شمارهٔ ۶۴ دورهٔ ۱۶ پاییز ۱۳۹۹، ۴۱ـ۵۱.

اصغرپور، محمدجواد (۱۳۷۷)، تصمیم‌گیری چندمعیاره، تهران: دانشگاه تهران.

آفتابی، نوید (۱۳۹۷)، یک مدل مدیریت امنیت اطلاعات برای کاهش ریسک‌های

احتمالی در سازمان‌های مبتنی بر فناوری اطلاعات، *پایان‌نامهٔ کارشناسی ارشد گرایش سیستم‌های اقتصادی و اجتماعی*، دانشکدهٔ مهندسی صنایع دانشگاه صنعتی شریف. بازیابی از https://ganj.irandoc.ac.ir

پیکری، ح؛ بنازاده، ب (۱۳۹۷)، رابطهٔ آگاهی از امنیت اطلاعات با قصد نقض امنیت اطلاعات با نقش میانجی هنجارهای فردی و خودکنترلی عنوان مکرر: قصد نقض امنیت اطلاعات، *پژوهش‌های راهبردی مسائل اجتماعی ایران*، سال هفتم، شمارهٔ پیاپی ۲۳، شمارهٔ چهارم، زمستان ۱۳۹۷.

خیری، سعید (۱۳۹۴)، شناسایی، تحلیل و رتبه‌بندی عوامل مؤثر کلیدی در پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان‌های حاکمیتی (مطالعهٔ موردی: سازمان بنادر و دریانوردی)، *صنعت حمل‌ونقل دریایی*، پاییز ۱۳۹۵، دورهٔ ۲، شمارهٔ ۳، ۳۶ـ۴۶.

رضایی، علی و همکاران (۱۳۹۷)، عوامل مؤثر بر اثربخشی سیستم مدیریت امنیت اطلاعات، *مجلهٔ مدیریت توسعه و تحول*، ۳۳، ۷۳ـ۸۲.

سازمان ملی استاندارد ایران (۱۳۹۲)، استاندارد ایران ـ ایزو ـ آی‌ای‌سی ۲۷۰۱۴: فناوری اطلاعات، فنون امنیتی، حاکمیت امنیت اطلاعات، سازمان ملی استاندارد ایران.

عیسی زاده، ع (۱۳۹۴)، رتبه‌بندی عوامل کلیدی موفقیت در پیاده‌سازی سیستم مدیریت امنیت اطلاعات، کنفرانس بین‌المللی پژوهش‌های نوین در مدیریت و مهندسی صنایع. بازیابی از https://civilica.com/doc/435237/

فقیهی، ا؛ علیزاده، م (۱۳۸۴)، روایی در تحقیق کیفی، *فرهنگ مدیریت*، ۱۳۸۴ شمارهٔ ۹.

نورائی، فرزاد (۱۳۹۱)، بررسی و شناسایی عوامل موفقیت استقرار سیستم مدیریت امنیت اطلاعات ISMS در ایران (مطالعهٔ موردی: بانک دی)، *پایان‌نامهٔ کارشناسی ارشد در رشته مدیریت فناوری اطلاعات*، دانشگاه سیستان و بلوچستان.

Al-Ahmad, W., & Mohammad, B. (2012). CAN A SINGLE SECURITY FRAMEWORK ADDRESS INFORMATION SECURITY RISKS ADEQUATELY? International Journal of Digital Information and Wireless Communications (IJDIWC) 2(3), 222-230.

Allen, J. H. (2013). Security Is Not Just a Technical Issue. CERT.

Bobbert, Y., & Mulder, H. (2015). Governance Practices and Critical Success factors suitable for Business Information Security, in International Conference on Computational

Bowen, P., Hash, Joan, & Wilson, M. (2006). Information Security Handbook: A Guide forManagers. National

Carrow, E. (. (2014). Information Security - Governance & Practice.

CASPUK. (2022). https://casp-uk.net/casp-tools-checklists/. Retrieved from www.casp-uk.net.

CGI. (2016). IT Security Governance A holistic approach. © 2016 CGI GROUP INC.

de Oliveira Alves, G. d. (2006). Enterprise Security Governance; A practical guide to implement and control Information Security Governance (ISG).

Diesch, R., & et al. (2020). A comprehensive model of information security factors for decision-makers. Computers & Security 92 (2020) 101747. Retrieved from https://www.sciencedirect.com/

Erwin, E. J., & et al. (2011). Understanding Qualitative Metasynthesis: Issues and Opportunities in Early Childhood Intervention Research. Journal of Early Intervention 33(3), 186-200.

Gashgari, G., & et al. (2017). A Proposed Best-practice Framework for Information Security. IoTBDS 2017 - 2nd International Conference on Internet of Things, Big Data and Security (pp. 295-301). SCITEPRESS – Science and Technology Publications, Lda.

Haufe, K., & al, e. (2016). A process framework for information security management. International Journal of Information Systems and Project Management, 27-47. doi:10.12821/ijispm040402

ISO. (2022). https://www.iso.org/standard. Retrieved from https://www.iso.org.

ITGI. (2006). Information Security Governance: Guidance for Boards of Directors and Executive Management (2nd ed.). IT Governance Institute.

ITGI. (2008). Information Security Governance-Guidance for Information Security Managers. IT Governance Institute. Retrieved from www.itgi.org

Loeffen, F. (2019). ICT in Business-The development of an information security governance maturity model for Dutch hospitals. Master Thesis-Leiden Institute of Advanced Computer Science (LIACS).

Love, P., & et al. (2010). GTAG Information Security Governance. The Inistitute of Internal Auditors, 134.

ISACA. (2022). https://www.isaca.org/resources/cobit. Retrieved from https://www.isaca.org.

Maleh, Y., & et al. (2017). Towards A Capability Assessment Framework for Information Security Governance in Organization.

MIJNHARDT, F., & et al. (2016). ORGANIZATIONAL CHARACTERISTICS INFLUENCING SME INFORMATION SECURITY MATURITY. Journal of Computer Information Systems 56(2), 106-115.

National Cyber Security Summit Task Force (2004). Information Security Governance: a Call To Action, Coroprate Governance Report

Nazareth, L., & Choi, J. (2015). A system dynamics model for information security management. Information & Management Volume 52, Issue 1, 123-134.

Nicho, M. (2018). A Process Model for Implementing Information Systems Security Governance. Information and computer security [online], 26(1), 10-38. Retrieved from https://openair.rgu.ac.uk

Noblit, G., & Hare, R. (1988). Meta-ethnography: synthesizing qualitative studies.

Norman, A. A., & Yasin, N. M. (2013). Information systems security management (ISSM) success factor: Retrospection from the scholars. *African Journal of Business Management-Vol. 7(27)*, 2646-2656.

Paul Williams, A. (2001). Information Security Governance, Information Security Technical Report,6(3), 60–70.

Rastogi, R., & von Solms, R. (2004). Information Security Governance-A Re-Definition, Security Management, Integrity, and Internal Control in Information Systems,193, 223–236.

Sandelowski, M. (2007). Handbook for Synthesizing Qualitative Research. Springer Publishing Company.

Schinagl, S., & Shahim, A. (2019). What do we know about information security governance?“From the basement to the boardroom”:towards digital security governance. Information & Computer Security,Vol. 28 No. 2, 2020, 261-292. doi:10.1108/ICS-02-2019-0033

Tu, Z.,&Yuan, Y., 2014. Critical success factors analysis on effective information se- curity management: a literature review. In: 20th Americas Conference on Infor- mation Systems, pp. 1874–1886

Tu, C., & et al. (2018). Strategic value alignment for information security management: A critical success factor analysis. *Information and Computer Security, 26(2)*, 150-170.

Westby, J., & Allen, J. (2007). Governing for Enterprise Security (GES) Implementation Guide, Software Engineering Institute, CERT, (August), 1–17.

Williams, S., & et al. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. Electron Markets (2013) 23,341–354. doi:10.1007/s12525-013-0137-3

Zimmer, L. (2006). Qualitative meta-synthesis: a question of dialoguing with texts. Journal of Advanced Nursing53(3), 311-318. doi:10.1111/j.1365-2648.2006.03721.x