Journal of Information Technology Management
ISSN: 2008-5893
EISSN: 2423-5059
Vol. 9, No. 2; PP. 379 - 404
Summer 2017

University of Tehran
Faculty of Management

IT Security Management Implementation Model in Iranian Bank Industry

Mona Vanaki [1], Mohammad Reza Taghva [2],
Seyed Mohammad Taghi Taghavi Fard [3], Kamran Feizi [4]

Abstract: According to the complexity and differences between Iranian banks and other developed countries the appropriate actions to implement effective security management of information technology have not been taken. The aim of this study was to create a powerful model by selecting the appropriate security controls to protect information assets in the bank. In this model, at first the principle set for in ISO standard 27001, was extracted and then by further studies derived from best practices carried out in the world on the related subject from 2008 to 2016 using a qualitative descriptive method), points comply with information security management in the banking industry were added to it. With the study of Iranian banks in dealing with IT security management system and with help of action research tools, provisions which prevent the actual implementation of this standard was removed and finally a conceptual model with operating instructions and considering all the principles of information security management standard, as well as banking institutions focusing on the characteristics of Iran was proposed.

Key words: ***Asset, Banking, Information security management system certification, ISO 27001 standard.***

1. Ph.D. Candidate in IT, Allameh Tabatab'i University, Tehran, Iran
2. Associate Prof. in Industrial Management, Allameh Tabatab'i University, Tehran, Iran
3. Associate Prof. in Industrial Management, Allameh Tabatab'i University, Tehran, Iran
4. Prof. in Industrial Management, Allameh Tabatab'i University, Tehran, Iran

Submitted: 04 / September / 2016
Accepted: 14 / March / 2017
Corresponding Author: Mohammad Reza Taghva
Email: taghva@atu.ac.ir

مدیریت فناوری اطلاعات
Journal of Information Technology Management
دانشکدهٔ مدیریت دانشگاه تهران
دورهٔ ۹، شمارهٔ ۲
تابستان ۱۳۹۶
صص. ۴۰۴- ۳۷۹

مدل پیاده‌سازی مدیریت امنیت فناوری اطلاعات در صنعت بانکداری ایران

مونا ونکی[۱]، محمدرضا تقوا[۲]، سید محمد تقی تقوی فرد[۳]، کامران فیضی[۴]

چکیده: بر اساس پیچیدگی و تفاوت فرایندیِ بانک‌های ایرانی با سایر کشورهای توسعه‌یافته و در راستای پیاده‌سازی اثربخش مدیریت امنیت در حوزهٔ فناوری اطلاعات، تاکنون اقدام مناسبی انجام نشده است. از این رو هدف از اجرای این پژوهش، ارائهٔ مدل قدرتمند با انتخاب کنترل‌های امنیتی مناسب به‌منظور محافظت از دارایی‌های اطلاعاتی بانک‌هاست. در این مدل، ابتدا اصل‌های مندرج در استاندارد ایزو ۲۷۰۰۱ استخراج شد، سپس با مطالعهٔ بهترین تجربه‌های جهان دربارهٔ موضوع از سال ۲۰۰۸ تا ۲۰۱۶، از طریق روش توصیفی و کیفی، نکات منطبق بر مدیریت امنیت اطلاعات در صنعت بانکداری به آن اضافه شد. در ادامه با مطالعهٔ عملکرد بانک‌های ایرانی در خصوص برخورد با پیاده‌سازی نظام مدیریت امنیت فناوری اطلاعات به کمک ابزار اقدام‌پژوهی، بندهایی که مانع اجرایی شدن حقیقی این استاندارد می‌شد، حذف شدند و در نهایت یک مدل مفهومی، حاوی دستورالعمل‌های اجرایی با در نظر گرفتن کلیهٔ اصول استاندارد مدیریت امنیت اطلاعات و متمرکز بر ویژگی مؤسسه‌های بانکی ایران پیشنهاد شد.

واژه‌های کلیدی: استاندارد ایزو ۲۷۰۰۱، بانکداری، دارایی، گواهی‌نامهٔ مدیریت امنیت اطلاعات.

۱. دانشجوی دکتری مدیریت فناوری اطلاعات، دانشگاه علامه طباطبائی، تهران، ایران
۲. دانشیار گروه مدیریت صنعتی، دانشکدهٔ مدیریت و حسابداری، دانشگاه علامه طباطبائی، تهران، ایران
۳. دانشیار گروه مدیریت صنعتی، دانشکدهٔ مدیریت و حسابداری، دانشگاه علامه طباطبائی، تهران، ایران
۴. استاد گروه مدیریت صنعتی، دانشکدهٔ مدیریت و حسابداری، دانشگاه علامه طباطبائی، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹۵/۰۶/۱۴
تاریخ پذیرش نهایی مقاله: ۱۳۹۵/۱۲/۲۴
نویسندهٔ مسئول مقاله: محمدرضا تقوا
E-mail: taghva@atu.ac.ir

مقدمه

حیات سازمان‌ها ارتباط نزدیکی با سیستم اطلاعاتی آنها دارد (تاج فر، میمند و رضا سلطانی، ۱۳۹۳). اطلاعات در دنیای کنونی ارزشمندترین دارایی هر سازمان محسوب می‌شود و باید آن را کالای اساسی هر سازمان دانست (موسوی زنوز و حسن‌پور، ۱۳۹۴). همچنین طی دهه‌های اخیر بسیاری از شرکت‌ها و مؤسسه‌ها بخشی از کسب‌وکار خود (یا تمام آن) را به‌سمت خدمات بر خط[1] سوق داده‌اند. در این میان بانک‌ها نیز از این فناوری بهره برده‌اند (وثوق، تقوی فرد و البرزی، ۱۳۹۳). همچنین به‌دلیل آنکه بانک‌ها با تراکنش‌های مالی افراد سروکار دارند، باید به حفظ محرمانگی و امنیت دارایی‌های اطلاعاتی آنها بیشتر از سایر سازمان‌ها توجه شود. از این رو مدیریت هدفمند امنیت اطلاعات در بانک اهمیت ویژه‌ای دارد. البته ممکن است ابتدا حرکت بر اساس سیستم مدیریت امنیت اطلاعات آن هم منطبق بر استانداردهای اروپایی که تطابق کمتری با شرایط زیرساختی سازمان‌های ایرانی دارند، کمی دشوار به نظر برسد؛ اما با نگاهی عمیق‌تر می‌توان دریافت که استقرار این نظام بر اساس روش منحصربه‌فرد، تأثیر بسزایی در پیشگیری از حوادث اطلاعاتی دارد. در این وضعیت نبود مدل بهینه برای پیاده‌سازی مدیریت امنیت فناوری اطلاعات در بانک‌های ایرانی کاملاً مشهود است. در این خصوص استانداردها، چارچوب‌ها و تجربه‌های زیادی در حوزهٔ بین‌المللی ارائه شده است؛ اما آنچه اهمیت دارد، تمرکز این روش‌ها بر تعاریف و اصول مدیریت امنیت اطلاعات است، به‌طوری که حجم عظیمی از داده‌ها را به افراد منتقل می‌کند؛ حال آنکه حلقهٔ گم‌شده در این بخش، به مدل گام به گامی نیاز دارد که متخصصان حوزهٔ بانکی، متناسب با شرایط خود از آن بهره ببرند.

در این پژوهش تلاش شده است با طراحی مدل خلاقانه‌ای در سطوح معین و منطبق بر نیازهای صنعت بانکداری ایران، نسبت به اجرای صحیح این مدیریت در بانک‌های ایرانی، گامی مؤثر برداشته شود.

بیان مسئله

مدیریت امنیت اطلاعات، بخشی از سیستم مدیریت کلی و سراسری در هر سازمان است که بر پایهٔ رویکرد مخاطرات کسب‌وکار قرار دارد و هدف آن پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی، نگهداری و بهبود امنیت اطلاعات است (شالی، ۱۳۸۴). در صورت پیاده‌سازی صحیح این نوع مدیریت می‌توان با کاهش ریسک‌های پیرامونی به‌عنوان عامل مهم، در تضمین سطح امنیتی تعریف‌شده، نقش بسزایی را ایفا کرد (آستروسکا و مازور، ۲۰۱۵). در صورتی که

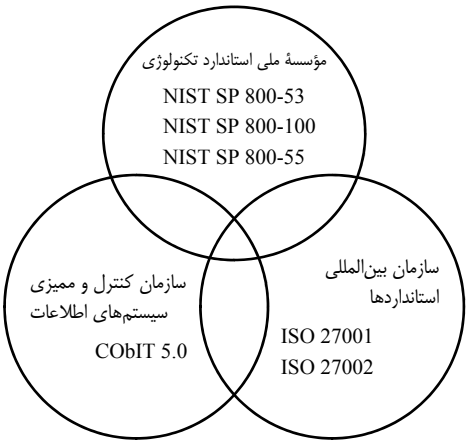
1. Online

سازمان مد نظر سیستم بانکی باشد، به‌دلیل حساسیت فراوان در امنیت کسب‌وکار و گردش مالی (عباسی، راج کامال، جوس و فرانسیس، ۲۰۱۵)، اهمیت به‌کارگیری این مدیریت دوچندان می‌شود. با در نظر گرفتن این موضوع که ایجاد و حفظ اعتماد میان بانک و مشتریان آن ضرورت دارد و اطلاعات به‌موقع و معتبر برای اجرای سرمایه‌گذاری‌ها و تصمیم‌گیری‌های صحیح لازم است، چنانچه اطلاعات افشا، حذف یا دستکاری شوند یا در صورت نیاز در دسترس نباشند، درآمدها و سرمایه‌های بانک تحت تأثیر قرار گرفته و پیامدهای جبران‌ناپذیری را دربرخواهد داشت (جراحی و عظیمی، ۱۳۸۷). همچنین پیاده‌سازی سیستم مدیریت امنیت در بخش فناوری اطلاعات بانک‌ها به‌دلیل نوع دارایی‌ها که از جنس اطلاعات مالی هستند، تفاوت در زیرساخت تبادل اطلاعات، نوع فرایندهای به‌کارگرفته‌شده و نیز ساختار داده‌ها در بانک، در مقولهٔ امنیت متفاوت از سایر سازمان‌هاست. در این میان، جامعهٔ بانکداران در تلاش هستند تا بدانند چگونه می‌توان برنامه‌های امنیت اطلاعات را توسعه داد (کاریدا، تسوهو و کوکولاکیز، ۲۰۱۵). به همین دلیل، بانک‌ها باید برنامهٔ امنیت اطلاعات خود را بر اساس اندازهٔ ساختار، پیچیدگی و نوع استفاده از فناوری انتخاب کنند، سپس از طریق مدل منحصربه‌فردی به مدیریت آن بپردازند (دستورالعمل میانی ایجاد استاندارد برای حفاظت از اطلاعات مشتریان[1]، ۲۰۰۱).

در این خصوص دستورالعمل‌های بسیاری برای رعایت استانداردهای حفاظت از اطلاعات از سوی نهادهای نظارتی در اختیار بانک‌ها، شرکت‌های اصلی بانک و سایر شرکت‌های تابعهٔ بانکی قرار می‌گیرد. بر اساس این دستورالعمل‌ها، بانک باید برنامهٔ امنیت اطلاعات (ISP)[2] معتبر را طوری اجرا کند که شامل حراست اداری، فنی و فیزیکی مناسب بر اساس اندازه و پیچیدگی‌های بانک، ماهیت یا دامنهٔ فعالیت آن باشد. این برنامه باید به نوعی طراحی شود که متضمن حفظ امنیت اطلاعات بوده و دارایی‌های اطلاعاتی را در برابر هرگونه تهدید پیش‌بینی‌ناپذیر یا خطرهای امنیتی حفظ کند. در این میان، ارزیابی ریسک یک روش منطقی برای تعیین اندازهٔ کمی و کیفی خطرها و بررسی پیامدهای بالقوهٔ ناشی از حوادث احتمالی روی افراد، اسناد، تجهیزات و محیط است (کوآ و سانگ، ۲۰۱۶). شایان ذکر است، مدیریت امنیت اطلاعات شامل سه استاندارد برای توسعهٔ هر برنامهٔ امنیتی است. این سه استاندارد عبارت‌اند از: نیست[3]، کوبیت[4] و ایزو[5] که در شکل ۱ شمایی کلی از آن مشخص شده است.

---

1. Interagency Guidelines Establishing Standards for Safeguarding Customer Information
2. Information Security Plan
3. National Institute of Standard and Technology (NIST)
4. Control Objective for Information and related Technology (CObIT)
5. International Standard Organization (ISO)



شکل ۱. روابط میان استانداردها و چارچوب‌های موجود در حوزهٔ امنیت اطلاعات

منبع: مدیری و شیخ‌پور (۲۰۱۲)

هر یک از این استانداردها و دستورالعمل‌ها، تعریف‌ها و عملکرد مخصوص به خود را دارند که باید با بهره‌مندی هوشمندانه از نکات کلیدی آنها، سیستم مدیریت امنیت اطلاعات را پیاده‌سازی کرد (میلر، ۲۰۱۶). در نتیجه هدف از تدوین مقالهٔ حاضر، ارائهٔ یک مدل کامل با الهام از مفاهیم مدیریت امنیت اطلاعات بر اساس ساختار بانک‌های ایرانی، به‌منظور پیاده‌سازی گام به گام تمام مراحل تا زمان انجام ممیزی (هینسون، ۲۰۰۷) است.

شایان ذکر است برای تعریف یک مدل می‌توان از کوشش‌های مشابهی که برای استقرار نظام مدیریت امنیت در مقالات معتبر بیان شده است، بهره برد. بر این اساس افزون بر ۱۰۲ مقاله از میان نوشته‌ها و تحقیق‌های به‌دست‌آمده از سال ۲۰۰۸ تا ۲۰۱۶ که عنوان آنها تطابق و همخوانی بیشتری با مقولهٔ مدیریت امنیت اطلاعات داشت، انتخاب شدند.

اهداف و ضرورت‌های پژوهش

طراحی مدل مدیریت امنیت اطلاعات بر اساس ساختار، روش‌ها و فرایندهای بانک، فعالیتی است که از طریق آن می‌توان سه مفهوم خاص محرمانه‌بودن اطلاعات، صحت اطلاعات و در دسترس بودن اطلاعات (تاج فر و همکاران، ۱۳۹۳) را تضمین کرد. در این خصوص دریافت گواهی‌نامهٔ مدیریت امنیت اطلاعات توسط تعداد محدودی از بانک‌ها و مؤسسه‌های مالی (سایت

بانک مرکزی، ۱۳۹۶)[1] به‌عنوان حرکتی نمادین، بدون توجه به حرکت در عمق و اجرایی کردن مستمر دستورالعمل‌های مرتبط با این موضوع، تنها مواردی هستند که تا کنون انجام شده است.

بر اساس نظر برخی ممیزان استاندارد ایزو ۲۷۰۰۱ مانند تروزا[2] (ممیز بانک کلارین[3] و حسابرس فیلیپین)، قوانین و مقررات در هر سازمان، موجب تکامل ریسک‌های مرتبط با امنیت اطلاعات می‌شود. همچنین برای پیاده‌سازی مؤثر این سیستم مدیریتی، ابتدا باید مفاهیم کتابخانهٔ زیرساخت فناوری اطلاعات که نشئت‌گرفته از بهترین تجربهٔ خدمات مبتنی بر فناروی اطلاعات است (مدیری و شیخ‌پور، ۲۰۱۲) در کلیهٔ سطوح اجرایی شود. همچنین بر اساس تحقیقات هُنان در سال ۲۰۱۰ تحت عنوان «پیاده‌سازی ایزو ۲۷۰۰۱ در دنیای واقعی»[4]، افزون بر ۶۰۰۰ سازمان جهانی به دریافت این گواهی‌نامه نائل شده‌اند. در این خصوص بر اساس نظرسنجی از سه نفر از مدیران کلیدی برخی شرکت‌ها مانند نیوتن[5] مدیر عامل شرکت بانکر[6]، تور[7] مدیر مسئول شرکت CSIRT و بروفی[8] مدیر عامل شرکت گواهی‌نامهٔ اروپایی، بزرگ‌ترین چالش شرکت‌ها در مواجهه با پیاده‌سازی این استاندارد، پیروی نکردن از تغییر بر اساس وضعیت سازمان و مقاومت در برابر تغییرات ناشی از پیاده‌سازی این مدیریت است. در این وضعیت، هر چه تجربه‌ها و قوانین پیاده‌سازی این نوع مدیریت بر اساس استاندارد، مطابقت کمتری با برخی ساختارها و مقررات موجود در سازمان‌های هدف داشته باشد، این نوع مدیریت تغییر[9] دشوارتر خواهد شد. همچنین با عنایت به اینکه اغلب رویکردهای مدیریت امنیت اطلاعات در قالب گزارش‌های فنی، الزاماتی را برای پیاده‌سازی دربردارند، گمان می‌رود پیروی از خط‌مشی مدون و اجرای مراحل آن، موجب پیاده‌سازی صحیح این مدیریت در سازمان می‌شود. با وجود این تصور، از آنجا که این استانداردها از تعریف‌ها، ساختارها و بهترین تجربه‌های به‌دست‌آمده از سازمان‌های اروپایی و آمریکایی الهام گرفته‌اند، سازگاری با آنها در کشورهای خاورمیانه از جمله ایران و مطابقت دادن فرایندها و قوانین یک سازمان داخلی مانند بانک در راستای اجرای آن، بسیار دشوار به نظر می‌رسد. به‌دلیل این تفاوت، با وجود مشابهت در شرح وظایف اصلیِ (کالین،۲۰۰۰) بانک‌های داخلی و خارجی، نمی‌توان روند واحدی برای پیاده‌سازی این مهم برای آنها در نظر

1. www.cbi.ir
2. Arhnel Klyde S.Terroza
3. Clarien
4. Implementing ISO 27001 in the real world
5. Peregrine Newton
6. Bunker
7. Hon Van Thoor
8. Michel Brophy
9. Change Managment

گرفت و ایجاد یک مدل بومی، ضروری به نظر می‌رسد. در نتیجه، جنبهٔ نوآوری و خلاقیتِ این پژوهش به‌منظور طراحی و معرفی مدلی ساده و کارا که با پیروی از آن بتوان علاوه بر تشویق سازمان‌ها در حرکت به‌سوی این هدف، در پیاده‌سازی کامل و جامع سیستم مدیریت امنیت اطلاعات در راستای پیشگیری از وقوع رخدادهای احتمالی، امنیت سیستم‌های ارائه‌دهندهٔ خدمات، قابلیت اطمینان سیستم‌ها و دامنهٔ خدمات بانکی (نادری خورشیدی و قاسمی‌نژاد، ۱۳۹۳) گام برداشت، بسیار مشهود است. بر اساس تحقیقات به‌عمل‌آمده و مطالعهٔ وب‌سایت بانک‌ها، از ۳۵ بانک و مؤسسهٔ مالی داخلی مندرج در جدول ۱، تا کنون اغلب گواهی‌نامه‌های مدیریت امنیت اطلاعات در بخش حوزهٔ بانکداری از طریق مؤسسه‌های خارجی دریافت شده و تنها یک بانک این گواهی‌نامه را به‌صورت داخلی دریافت کرده است.

جدول ۱. اسامی بانک‌های داخلی بررسی‌شده[1]

ردیف	طبقهٔ بانک/ مؤسسهٔ مالی	تعداد	نام بانک	دریافت گواهی‌نامه	نام شرکت	داخلی/ خارجی	سال دریافت	اعتبار
۱	بانک‌های تجاری دولتی/ غیر دولتی/ تخصصی/قرض‌الحسنه / مؤسسه‌های اعتباری	۳۲	-	اطلاعاتی موجود نیست				
۲	بانک‌های غیردولتی	۳	ملت	بله (در حوزهٔ بانکداری اینترنتی)	DNV انگلستان	خارجی	۱۳۹۰	۱۳۹۳
			شهر	بله (در حوزهٔ بانکداری الکترونیک)	ACS انگلستان	خارجی	۱۳۹۲	۱۳۹۵
			صادرات	بله (در حوزهٔ فناوری اطلاعات)	مرکز راهبردی افتا	داخلی	۱۳۹۳	۱۳۹۵

بر اساس اعلام سازمان فناوری اطلاعات ایران و مرکز نما[2]، تا زمان نگارش این مقاله تنها دو شرکت داخلی، پروانهٔ فعالیت در نظام ملی مدیریت امنیت اطلاعات در زمینهٔ ارائهٔ خدمات ممیزی را دریافت کرده است. با توجه به موارد مطرح‌شده، بانک‌های داخلی به‌عنوان مراکزی که ساختارهای منحصربه‌فرد خود را دارند و نیز، در کنار شباهت‌های موجود با بخش‌های زیرساخت

۱. تعداد بانک‌ها از سایت بانک مرکزی به نشانی www.cbi.ir به‌دست آمده است و نتایج مندرج در جدول از واحد مرتبط در آن بانک‌ها و مؤسسه‌ها استخراج شده است.

۲. نظام مدیریت امنیت (http://nama.ito.gov.ir)

بین‌المللی، دارای تفاوت‌های عمده در حوزهٔ امنیت هستند، انتخاب آن برای جامعهٔ آماری، از جمله ضرورت‌های این پژوهش به‌شمار می‌رود.

شاخص‌های این پژوهش با مطالعهٔ مقالات بر اساس حوزه‌های اصلی مورد نیاز در پیاده‌سازی صحیح یک سیستم مدیریت امنیت اطلاعات و با الهام از ۱۸ سرفصل نسخهٔ جدید استاندارد ایزو ۲۷۰۰۱ انتخاب شده است. حوزه‌های یاد شده بر اساس این تفکر که برقراری امنیت به موارد زیر نیاز دارد، دسته‌بندی شده‌اند:

۱. مدیریت و کنترل صحیح؛
۲. بررسی تهدیدها و آسیب‌ها؛
۳. بررسی رخدادهای امنیتی به وقوع پیوسته؛
۴. ارائهٔ طرح‌های مدون در خصوص بازیابی و احیای سیستم‌ها و تداوم خدمات پس از وقوع بحران‌های امنیتی؛
۵. نظارت و مدیریت بر ریسک‌ها.

شایان ذکر است که هر یک از این بخش‌ها، دربرگیرندهٔ زیربخش‌هایی هستند که به‌دقت بررسی شده‌اند.

پیشینهٔ پژوهش

استاندارد BS ۷۷۹۹[1] در سال ۱۹۹۵ برای نخستین بار توسط گروه استانداردهای انگلستان (BSI)[2] به‌وجود آمد. این استاندارد که توسط مجموعهٔ صنعت و تجارت دولت بریتانیا نوشته شده، از چندین بخش تشکیل شده است. نخستین بخش که شامل بهترین تجربه‌های مدیریت امنیت اطلاعات است، در سال ۱۹۹۸ بازبینی شد. پس از بحث و تبادل نظر بسیار بین صاحبان استاندارد در جهان، این استاندارد در سال ۲۰۰۰ توسط بنیاد ایزو با عنوان ایزو ۱۷۷۹۹ انطباق لازم را پیدا کرد و عنوان «تکنولوژی اطلاعات ـ کد تجربی مدیریت امنیت اطلاعات» را کسب کرد (برنر، ۲۰۰۷). این استاندارد در ژوئن سال ۲۰۰۵ بازبینی شد و در سال ۲۰۰۷ با عنوان ایزو ۲۷۰۰۲ در سری استانداردهای ایزو ۲۷۰۰۰ قرار گرفت.

بخش دوم BS ۷۷۹۹ برای نخستین بار در سال ۱۹۹۹ و با کد «BS ۷۷۹۹ – نسخهٔ ۲» با عنوان «سیستم‌های مدیریت امنیت اطلاعات ـ مشخصات، به انضمام راهنمای کاربرد» منتشر شد (برنر، ۲۰۰۷).

---

1. British Standard
2. British Standards Institution (BSI Group)

۲- BS ۷۷۹۹ بر نحوهٔ پیاده‌سازی سیستم مدیریت امنیت اطلاعات تمرکز دارد. این استاندارد بعدها به استاندارد ایزو ۲۷۰۰۱ تبدیل شد. نسخهٔ ۲۰۰۲ استاندارد ۲- BS ۷۷۹۹ چرخهٔ «برنامه‌ریزی، اجرا، بررسی، پیاده‌سازی» (چرخهٔ دمینگ یا PDCA) را معرفی کرد که بر محور استانداردهای کیفیت مثل ایزو ۹۰۰۰ بنا شده بود (مدیری و شیخ‌پور، ۲۰۱۲).

در نوامبر ۲۰۰۵ این استاندارد توسط بنیاد ایزو با ایزو ۲۷۰۰۱ منطبق شد. ایزو ۲۷۰۰۱ قسمت ۳ نیز در سال ۲۰۰۵ منتشر شد که مدیریت تحلیل خطر را پوشش می‌داد. این استاندارد نیز بعدها با ایزو ۲۷۰۰۱ منطبق شد (گرین می‌یر، ۲۰۰۶).

شرکت‌های داخلی ایالات متحدهٔ آمریکا، این استاندارد شناخته‌شده و بین‌المللی را به‌کندی به‌کار گرفتند (گرین می‌یر، ۲۰۰۶)؛ زیرا درک این استاندارد و پیروی از آن بسیار دشوار بود (برونو و بریتز، ۲۰۰۶). به همین دلیل راهنمایی‌هایی برای اجرای گواهی ایزو ۲۷۰۰۱ ارائه شد. البته آگاهی از این استانداردها با کمبودهای خاص خود همراه است (وایولینو، ۲۰۰۶) و بانک‌ها با این استانداردها کمتر سازگار شده‌اند. در واقع، تا سال ۲۰۰۹ حتی یک بانک کوچک برای این استاندارد ثبت نام نکرد (اِسترِف، ۲۰۰۹). اگرچه این استاندارد بیانیهٔ قابل اجرایی داشت؛ به‌طور مستقیم با بانک‌ها سازگار نبود. برای مثال، اغلب بانک‌ها نرم‌افزارهای کلان خود را برنامه‌نویسی نمی‌کنند؛ بلکه کارکرد نرم‌افزار مرتبط را انتخاب کرده و شرکت سومی آن را اجرا می‌کند. حال آن که در استانداردهای ایزو، بر توسعهٔ نرم‌افزار و روند نگهداری آن تأکید فراوانی شده است. آنچه که موجب مشخص شدن شکاف علمی میان نظریه و اجرا بر مبنای استاندارد و عدم درک صحیح ارتباطی این دو موضوع با هم می‌شود، آن است که به نظر می‌رسد، از استانداردها برای سنجش و ارزیابی استفاده می‌شود، در نتیجه بهره‌مندی از آنها در مقولهٔ پیاده‌سازی، تلاش بیهوده‌ای است. این استانداردها در برخی از زیرشاخه‌های خود، اصول و الزامات پیاده‌سازی را بیان کرده‌اند که با تلفیق آنها با بهترین تجربه‌ها و تطبیق آنها با شرایط یک سازمان، می‌توان به مدلی بومی و کارا در این خصوص دست یافت.

در ادامهٔ پژوهش، از طریق مطالعات کتابخانه‌ای در دانشگاه علامه طباطبائی، پایان‌نامه‌های مربوط به حوزهٔ مدیریت امنیت بررسی شدند که اهم موضوعات مشابه با عنوان پژوهش، در جدول ۲ درج شده است. با بررسی پیشینهٔ پژوهش، مشاهده می‌شود که اغلب موضوعات، علی‌رغم پرداختن به سیستم مدیریت امنیت، روش معین و منحصربه‌فردی برای حرکت به سمت هدف نهایی این سیستم در بانک‌ها ارائه نکرده‌اند. در نتیجه ضرورت نیاز به تعریف این مدل، در کانون توجه قرار می‌گیرد.

جدول ۲. گردآوری پایان‌نامه‌های مبتنی بر موضوع مدیریت امنیت دانشگاه علامه طباطبائی

ردیف	عنوان پایان‌نامه	محقق	مقطع تحصیلی ـ سال
۱	ارائهٔ مدلی برای سنجش میزان آمادگی سازمان برای پیاده‌سازی سیستم مدیریت امنیت اطلاعات	شهیدی (۱۳۸۶)	کارشناسی ارشد
۲	تحلیل فاصلهٔ مدیریت امنیت مؤسسهٔ تحقیقاتی صنعتی متـرا، نسبت به استاندارد سیستم مدیریت امنیت اطلاعات با استفاده از رویکرد فازی	فکری ازگمی (۱۳۹۰)	کارشناسی ارشد
۳	رابطهٔ فرهنگ سازمانی با مدیریت امنیت اطلاعات در بانک ملی ایران	عاشوری زاده (۱۳۹۱)	کارشناسی ارشد
۴	نقش پیاده‌سازی کتابخانهٔ زیرساخت فناوری اطلاعات و سیستم مدیریت امنیت اطلاعات در تداوم خدمات فناوری اطلاعات	جعفرنژاد ثانی (۱۳۹۲)	کارشناسی ارشد
۵	ارزشیابی وضعیت عملکرد مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مستقر در شهر تهران بر اساس استاندارد بین‌المللی ایزو ۲۷۰۰۲	ملک الکلامی (۱۳۸۹)	کارشناسی ارشد

پیشینهٔ نظری

برای استحکام مدل می‌توان از تلاش‌های مشابهی که برای استقرار نظام مدیریت امنیت در مقالات معتبر بیان شده است، استفاده کرد. استانداردهای ایمنی اطلاعات، برگرفته‌شده از سازمان استانداردهای بین‌المللی ایزو ۲۷۰۰۱ را استاندارد مدیریت برای امنیت اطلاعات معرفی می‌کنند که آن را مؤسسهٔ استاندارد بریتانیا ارائه کرده و توسط ایزو اصلاح و پذیرفته شده است (استاندارد امنیت اطلاعات[1] ۲۷۰۰۱، ۲۰۰۵). در واقع، ایزو ۲۷۰۰۱ یک استاندارد امنیت اطلاعات است که به‌عنوان روشی برای حفظ اطلاعات مشتریان، شرکا و افراد مشغول به کار در سازمان‌ها طراحی شده و به‌صورت مجموعه‌ای از کنترل‌های امنیت اطلاعات بین‌المللی به رسمیت شناخته شده است (برنر، ۲۰۰۷).

1. Information Security Standard

شرکت‌های داخلی ایالات متحدهٔ آمریکا، این استاندارد شناخته‌شده و بین‌المللی را به‌کندی به‌کار گرفته‌اند (گرین می‌یِر، ۲۰۰۶). این مسئله از آنجا نشئت می‌گیرد که درک این استاندارد و پیروی از آن بسیار دشوار است (برونو بریتز، ۲۰۰۶).

طبق قوانین استاندارد پردازش اطلاعات فدرال (FIPS)[1] برای پیاده‌سازی حداقل شرایط در امنیت اطلاعات، باید ۱۷حیطهٔ مرتبط با امنیت رعایت شود.

مؤسسهٔ «نیست»، تا کنون نشریه‌های متعددی برای کمک به سازمان‌ها به‌منظور ایجاد امنیت اطلاعات ارائه کرده است (وبگاه نیست، ۲۰۰۷).

برای استحکام مدل می‌توان از تلاش‌های مشابهی که برای استقرار نظام مدیریت امنیت در مقالات معتبر بیان شده است، مانند چارچوب کوبیت در امنیت اطلاعات و پیشگیری از جرایم سایبری (ولدن، والورد و تالا، ۲۰۱۵)؛ ارزیابی ریسک‌های حاصل از تعامل کاری در سازمان‌ها (کوآ و سانگ، ۲۰۱۶) و مروری بر ساختار مدیریت امنیت اطلاعات، بهره برد.

پیشینهٔ تجربی

از میان نوشته‌ها و تحقیقات به‌دست‌آمده از سال ۲۰۰۸ تا ۲۰۱۶ که عنوان آنها تطابق و همخوانی بیشتری با مقولهٔ مدیریت امنیت اطلاعات داشت، ۱۰۲ مقاله از ۵۸ نشریه بررسی شد که در نهایت علاوه بر در نظر گرفتن بخشی به‌عنوان «اصطلاحات حوزهٔ امنیت اطلاعات» بر اساس انطباق موضوع‌ها با سرفصل‌های استانداردهای امنیتی مانند سری ایزو ۲۷۰۰۰، مباحث بدون توجه به بخش اصطلاحات امنیت اطلاعات، به پنج بخش اصلی طبقه‌بندی شدند که در جدول ۳ نشان داده شده است: ۱. حوادث امنیتی، ۲. تهدیدها و آسیب‌ها، ۳. ممیزی و مدیریت ریسک، ۴. کنترل و مدیریت امنیت اطلاعات و ۵. طرح بازیابی و تداوم خدمات.

نتایج به‌دست‌آمده از این جدول نشان می‌دهد در بخش ۴ با عنوان کنترل و مدیریت امنیت اطلاعات، صرفاً دو مقاله (برگرفته از پایان‌نامه‌های مقطع دکتری) به‌صورت کلی به مقولهٔ مدل‌های امنیت اطلاعات پرداخته است که در مجموع ۸ درصد از مقالات طبقهٔ نام‌برده و ۳ درصد از کل مقالات مروری را به خود اختصاص داده است. همچنین در این طبقات، روش و مدل منحصربه‌فردی در خصوص نحوهٔ پیاده‌سازی بر اساس شرایط سازمان‌ها بیان نشده است. پس از انجام این مطالعات، تمام تحقیقات به مطالعات موردی و اجرایی در زمینهٔ پیاده‌سازی مدیریت امنیت اطلاعات در مراکز علمی و دانشگاهی معطوف شد. در نهایت می‌توان اذعان داشت که در کنار موضوعاتی از قبیل ارائهٔ مدلی برای سنجش میزان آمادگی سازمان‌ها در راستای پیاده‌سازی

1. Federal Information Processing Standard (FIPS)

سیستم مدیریت امنیت اطلاعات، تحلیل فاصلهٔ مدیریت امنیت مؤسسه‌ها نسبت به استاندارد سیستم مدیریت امنیت، رابطهٔ فرهنگ سازمانی با مدیریت امنیت اطلاعات، نقش پیاده‌سازی کتابخانهٔ زیرساخت فناوری اطلاعات و سیستم مدیریت امنیت اطلاعات در تداوم خدمات فناوری اطلاعات، ارزشیابی وضعیت عملکرد مدیریت امنیت اطلاعات و ... در پژوهش‌های انجام شده در دانشگاه‌ها، فقط دو رسالهٔ دکتری به این مسئله در حوزهٔ فرهنگی پرداخته‌اند؛ نخستین رساله در دانشگاه آفریقای جنوبی در سال ۲۰۰۶ با عنوان «یک مدل احیاکننده و آگاهی‌بخش امنیت اطلاعات برای صنعت» و دومی در دانشگاه فناوری کوینزلند استرالیا در سال ۲۰۱۱ با عنوان «مدیریت امنیت اطلاعات: مطالعهٔ موردی فرهنگ امنیت اطلاعات». در نتیجه، به طراحی مدلی برای پیاده‌سازی مدیریت امنیت فناوری اطلاعات در صنعت بانکداری ایران، نیاز داریم.

جدول ۳. طبقه‌بندی مقالات

طبقه‌بندی موضوعات	تعداد مقالات	درصد ارتباط موضوع به موضوع طبقات	درصد ارتباط موضوع به کل موضوع طبقات
۱. اصطلاحات امنیت اطلاعات			
۱.۱. امنیت	۴	۱۱/۱	
۱.۲. امنیت سایبری	۸	۲۲/۲	
۱.۳. رخداد	۵	۱۳/۹	
۱.۴. تهدید	۴	۱۱/۱	
۱.۵. آسیب	۱	۲/۸	درصد این بخش به دلیل اشتراک با سایر بخش‌ها قابل محاسبه نیست.
۱.۶. ریسک	۵	۱۳/۹	
۱.۷. کلاهبرداری	۳	۸/۳	
۱.۸. جرم	۲	۵/۶	
۱.۹. دزدی	۳	۸/۳	
۱.۱۰. شبکهٔ بات	۱	۲/۸	
جمع	۳۶	۱۰۰	
۲. رخداد امنیتی			
۲.۱. رخداد و تهدید	۳	۶۰	۴/۵
۲.۲. افزایش آسیب‌ها	۱	۲۰	۱/۵
۲.۳. عوامل مؤثر در رخدادهای امنیت اطلاعات	۱	۲۰	۱/۵
جمع	۵	۱۰۰	۷/۶

ادامهٔ جدول ۳

طبقه‌بندی موضوعات	تعداد مقالات	درصد ارتباط موضوع به موضوع طبقات	درصد ارتباط موضوع به کل موضوع طبقات
۳. تهدیدها و آسیب‌ها			
۳.۱. تهدیدهای محلی	۳	۱۳/۰	۴/۵
۳.۲. روش‌های حمله	۱	۴/۳	۱/۵
۳.۳. شبکهٔ بات	۱	۴/۳	۱/۵
۳.۴. مقابله با بدافزار	۳	۱۳/۰	۴/۵
۳.۵. کلاهبرداری و جرایم رایانه‌ای	۲	۸/۷	۳/۰
۳.۶. تشخیص و پیشگیری از کلاهبرداری	۱	۴/۳	۱/۵
۳.۷. سرقت هویت	۳	۱۳/۰	۴/۵۵
۳.۸. تهدیدهای امنیتی فضای سایبر	۹	۳۹/۱	۱۳/۶
جمع	۲۳	۱۰۰	۳۴/۸
۴. کنترل و مدیریت امنیت اطلاعات			
۴.۱. کنترل‌های عمومی	۶	۲۴	۹/۱
۴.۲. کنترل‌های سازمانی	۴	۱۶	۶/۱
۴.۳. کنترل‌های برنامه‌های کاربردی	۲	۸	۳/۰
۴.۴. قوانین حکومتی	۷	۲۸	۱۰/۶
۴.۵. استاندارد امنیت	۲	۸	۳/۰
۴.۶. مدل‌های امنیت اطلاعات	۲	۸	۳/۰
۴.۷. قوانین مقابله با کلاهبرداری	۲	۸	۳/۰
جمع	۲۵	۱۰۰	۳۷/۹
۵. طرح مقابله با بحران و تداوم خدمات			
۵.۱. نقشهٔ راه و نکات عمومی	۱	۲۰	۱/۵
۵.۲. استراتژی دفاع	۱	۲۰	۱/۵
۵.۳. یادگیری و برنامه‌های آموزشی	۳	۶۰	۴/۵
جمع	۵	۱۰۰	۷/۶
۶. مدیریت ریسک و حسابرسی			
۶.۱. بازرسی سیستم‌های اطلاعاتی	۳	۳۷/۵	۴/۵
۶.۲. مدیریت ریسک	۵	۶۲/۵	۷/۶
جمع	۸	۱۰۰	۱۲/۱
جمع کلی	۱۰۲	۱۰۰	۱۰۰

فرضیه‌های پژوهش

با توجه به شرایط بانک‌های ایرانی در حوزهٔ امنیت اطلاعات و در راستای ایجاد مجموعهٔ ورودی قابل استناد برای طراحی مدل، چهار فرضیه به شرح زیر در نظر گرفته شده است:

۱. وجود یک مدل مشخص به‌منظور پیاده‌سازی مدیریت امنیت اطلاعات در بانک‌ها، در اجرای صحیح پیاده‌سازی این مدیریت، اثر مثبت، مستقیم و معناداری دارد.
۲. در نظر گرفتن روش مشخصی برای پیاده‌سازی مدیریت امنیت اطلاعات در بانک‌ها، در استمرار این مدیریت در سازمان‌ها، اثر مثبت، مستقیم و معناداری دارد.
۳. ایجاد یک سری فرایند به‌منظور انجام کارهای مرتبط با مدیریت امنیت اطلاعات، در پیاده‌سازی این مدیریت در بانک‌ها، اثر مستقیم، مثبت و معناداری دارد.
۴. دخیل‌کردن کارکنان در پیاده‌سازی مدیریت امنیت اطلاعات در بانک‌ها، در نتیجهٔ این پیاده‌سازی، اثر مستقیم دارد.

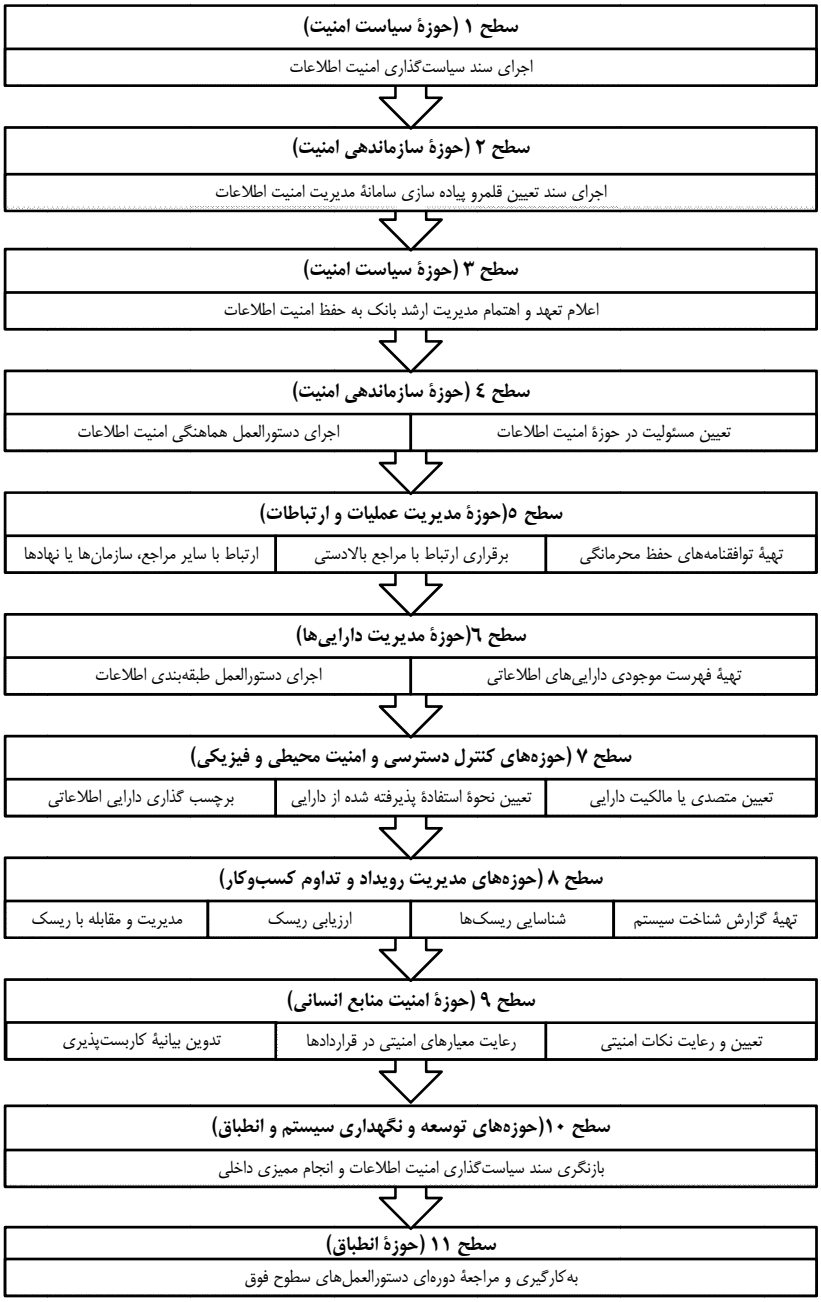
مدل مفهومی

پس از بررسی دقیق مطالب مطرح در پنج طبقهٔ اصلی بر اساس مقالات بیان‌شده در جدول ۳ و مطالعهٔ کامل استاندارد مدیریت امنیت اطلاعات ایزو ۲۷۰۰۱، پانزده شرط مندرج در این استاندارد با پنج مرحلهٔ کتابخانهٔ زیرساخت فناوری اطلاعات[1] در بخش‌های استراتژی، طراحی، انتقال، عملیات و بهبود مداوم خدمات (به‌دلیل پیاده‌سازی مدیریت امنیت در حوزهٔ فناوری اطلاعات و نیاز به ایجاد بستر اولیهٔ صحیح برای اجرای این مهم)، تلفیق شدند و پس از مشخص‌کردن مراحل اصلی و مهم، حذف ابهامات، جداسازی موارد اشتراکی و تکراری و اضافه‌کردن بخش‌های تخصصی مرتبط با بانک‌ها در مباحثی که مطالب به‌صورت کلی بیان شده است، دستورالعمل‌ها و فرم‌های لازم استخراج شد و یک طرح مبنایی ۱۱ سطحی بر اساس روش اقدام‌پژوهی به‌عنوان نقشهٔ راه، طراحی شد (شکل ۲) که این سطوح با مفاهیم موجود در مدل به‌منظور استقرار سیستم، سازگار شدند.

۱۱ سطح اجرای طرح مفهومی به‌عنوان نقشهٔ راه بر اساس روش اقدام‌پژوهی بدین صورت شکل گرفت؛ در مرحلهٔ «تشخیص مسئله»، بخش‌های مرتبط با سیاست‌گذاری، سازماندهی و هدف‌گذاری از مفاهیم استاندارد و کتابخانهٔ زیرساخت فناوری اطلاعات، استخراج شد و در سطوح ۱ تا ۳ قرار گرفت.

---

1. Information Technology Infrastructure Libraray (ITIL)



شکل ۲. سطح‌بندی اجرای مدل مفهومی به‌عنوان نقشهٔ راه

در مرحلهٔ «برنامه‌ریزی»، عناوین مرتبط با ایجاد برنامهٔ مشخص، شامل تعیین مسئولیت و ایجاد دستورالعمل هماهنگی، در سطح ۴ قرار گرفت. در مرحلهٔ «اقدام»، بخش‌های مدیریتی و عملیاتی که از لحاظ جایگاهی به انجام فعالیت‌های اجرایی نیاز دارند، در سطوح ۵ تا ۷ قرار گرفتند. در مرحلهٔ «ارزشیابی»، بررسی ریسک‌ها و نکته‌های مرتبط با مباحث امنیتی در سطوح ۸ و ۹ قرار گرفت و در نهایت، در مرحلهٔ «یادگیری و اصلاح» موارد نیازمند بازنگری و ممیزی به‌منظور تطبیق با اصول استاندارد، در سطوح ۱۰ و ۱۱ قرار گرفتند.

با آگاهی از این مراحل می‌توان این روش را در پژوهش مد نظر قرار داد و سازگاری آن با مراحل پیاده‌سازی مدل را شبیه‌سازی کرد.

نقشهٔ راه با سطح ۱ که مرتبط با حوزهٔ سیاست‌گذاری است، آغاز می‌شود. این مرحله که مهم‌ترین مرحله است، پایه و ستون اصلی مدل محسوب می‌شود. در این سطح سند سیاست‌گذاری سازمان با در نظر گرفتن اهداف استراتژیک حوزهٔ امنیت، تدوین شده و سایر بخش‌ها بر اساس آن شکل می‌گیرد. سطح ۲ که در حوزهٔ سازماندهی مدیریت امنیت اطلاعات است، قلمرو سازمان و محدودهٔ دارایی‌هایی را مشخص می‌کند که قرار است سیستم مدیریت امنیت (بر اساس سند سطح ۱) روی آن پیاده‌سازی شود. پس از تعیین قلمرو، دریافت تعهد از مدیر ارشد سازمان در سطح ۳، به‌منظور حمایت از این سیستم مدیریتی و نیز الزام سایر مسئولان به پای‌بندی به این تعهد قرار می‌گیرد که موجب دوام و پایداری مدل می‌شود. شایان ذکر است بدون حمایت مدیریت ارشد سازمان، ادامهٔ مراحل دشوار است، به همین دلیل، این مهم در سطوح ابتدایی بیان شده است. در سطح ۴، مسئولیت در حوزهٔ امنیت به گروه‌های مشخص واگذار شده تا هماهنگی‌های لازم در این بخش‌ها به‌منظور اجرای دستورالعمل استاندارد، بر اساس یک فرایند مشخص از سوی این افراد، صورت پذیرد. سطح ۵ که در حوزهٔ مدیریت عملیات و ارتباطات است، پس از تعیین مسئولیت‌ها در سطح ۴، راهکارهایی را برای برقراری ارتباطات امن افراد از طریق توافقنامه‌های منع افشای اطلاعات[1] و تدوین قوانین ارتباطی، بیان می‌کند. در سطح ۶ و ۷، پس از طی پنج سطح اولیه، ابتدا دارایی‌ها استخراج و فهرست‌بندی می‌شود و پس از تعیین طبقهٔ آنها در حوزهٔ دسترسی، نسبت به مشخص‌کردن نحوهٔ استفادهٔ پذیرفته شده از آنان بر اساس اصول امنیتی و تعیین متصدیان یا مالکان دارایی، از طریق روش برچسب‌گذاری اقدام خواهد شد. در این روش پس از جمع‌آوری اطلاعات بالا، موارد به‌صورت خلاصه و در قالب یک برچسب مشخص، روی هر دارایی الصاق می‌شود. در سطح ۸ که در حوزهٔ مدیریت رویداد و تداوم کسب‌وکار قرار می‌گیرد، شناخت سیستم از طریق بررسی میزان ریسک‌پذیری دارایی‌ها و

1. NDA

فرایندهای مرتبط با آنها، مقداردهی، ارزیابی و سرانجام تصمیم‌گیری برای پذیرش، رد، قبول، انتقال یا کاهش ریسک؛ از مهم‌ترین بخش‌های این مدل محسوب می‌شود. این بخش باید به‌صورت مستمر بازبینی شود و اتخاذ تصمیمات مناسب در حداقل زمان ممکن در دستور کار مسئولان تعیین‌شده قرار گیرد. در این صورت تداوم خدمات محقق خواهد شد. از آنجا که در مدل امنیت اطلاعات، انسان‌ها نقش مهمی دارند سطح ۹، به‌صورت مجزا به این مقوله اختصاص داده شده است. در این سطح نحوهٔ تعامل با کارکنان، مشتریان و پیمانکاران و نیروی انسانی در قراردادها، با ذکر جزئیات بیان می‌شود. همچنین یک بخش مهم از این سطح، بیانیهٔ کاربست‌پذیری است که در آن، اقدامات انجام‌شده در خصوص الزامات استاندارد ایزو ۲۷۰۰۱ ، به انضمام شواهدی که دلالت بر به‌کار بستن آن در سازمان دارد، به اختصار درج می‌شود. در سطح ۱۰، فرایندهای سطوح بالا، بازبینی و بازرسی شده و در نهایت پس از اعمال اصلاحات مورد نیاز و رفع ناهماهنگی‌های جزئی و کلی با استاندارد، در سطح ۱۱، ممیزی نهایی برای صدور گواهی‌نامه اجرایی می‌شود. شایان ذکر است ترتیب اجرای سطوح از بالا به پایین است و می‌توان دستورالعمل‌هایی را که در یک سطح قرار گرفته‌اند، به‌صورت موازی یا تقریباً همزمان به اجرا درآورد.

در این خصوص حوزه‌های اصلی منعکس‌شده در سطوح بالا، بر اساس مدل مفهومی جدول ۴ به تصویر کشیده شده است. پیاده‌سازی ۱۱ سطح عنوان‌شده در صورتی موفقیت‌آمیز خواهد بود که با ساختارهای تخصصی فناوری اطلاعات، همخوانی داشته باشد، از این رو ایجاد یک مدل مفهومی بسیار ضروری است. در این مدل محدودهٔ امنیت بر اساس مراحل کتابخانهٔ زیرساخت فناوری اطلاعات و کوبیت در چهار بخش و مراحل استقرار سیستم در یک محیط، بر اساس حوزه‌های عملیاتی ۱۱ سطح پیشین، مشخص شده است.

در ساختاری که در جدول ۴ به تصویر کشیده شده است، مرحلهٔ برنامه‌ریزی و ساماندهی با بخش سیاست در حوزهٔ امنیت اطلاعات، تلاقی داده شده است. این برخورد، از آنجا نشئت می‌گیرد که ایجاد برنامهٔ صحیح به‌تنهایی مؤثر نیست و اثربخشی آن زمانی کامل خواهد شد که این موضوع، به‌عنوان سیاست مدون از سوی مدیران ارشد سازمان، ابلاغ شود. بر این اساس نیاز به حمایت مدیریت ارشد سازمان، بیش از پیش احساس شده و در نتیجه این مهم به‌عنوان نقطهٔ تلاقی این دو رکن، مطرح شده است. حمایت مدیریت ارشد با علامت اختصاری FI1 نشانه‌گذاری شده است. سطر اول (برنامه‌ریزی و ساماندهی) با بخش سازماندهی امنیت نیز تلاقی دارد. این برخورد به این دلیل شکل گرفته است که برنامه‌ریزی تخصصی در حوزهٔ امنیت اطلاعات به سازماندهی مدیریتی نیاز دارد. در این خصوص انتخاب صحیح دامنه که در محل این

تلاقی قرار دارد، مشخص می‌کند که هر برنامه‌ریزی و سازماندهی از درون یک جامعهٔ هدف نشئت می‌گیرد. هر اندازه که این جامعه مشخص‌تر باشد یا به بیانی دیگر، دامنهٔ معینی را پوشش دهد، برنامه‌ریزی سهل‌تر خواهد بود. انتخاب صحیح دامنه نیز با علامت اختصاری FI2 نشانه‌گذاری شده است.

جدول ٤. مدل مفهومی تحقیق: مدلی برای پیاده‌سازی مدیریت امنیت اطلاعات دربانک‌ها

چرخهٔ بلوغ / محدودهٔ امنیت	مراحل استقرار سیستم									
	سیاست امنیت	سازماندهی امنیت	مدیریت دارایی	امنیت منابع انسانی	امنیت محیطی و فیزیکی	مدیریت عملیات و ارتباطات	کنترل دسترسی	توسعه و نگهداری سیستم	مدیریت رویداد	مدیریت تداوم کسب و کار	انطباق
برنامه‌ریزی و ساماندهی	FI1[1]	FI2	*I	I	I	I	I	I	I	I	×
اکتساب و پیاده‌سازی	×	×	FI3	I	I	I	I	I	FI3	FI3	×
خدمت رسانی و پشتیبانی	**×	×	×	I	I	I	I	I	I	I	×
نظارت و ارزیابی	I	I	I	I	I	I	I	I	I	I	FI4

FI1 حمایت مدیر ارشد؛ FI2 انتخاب صحیح دامنه؛ FI3 بومی‌سازی مراحل استاندارد؛ FI4 ممیزی رسمی؛
* مطابق با مراحل استاندارد رسمی ایزو ۲۷۰۰۱ و ** به‌معنای عدم تلاقی

روش مواجههٔ برخی سطرها با بخش‌های دیگر مدل (ستون‌های بعدی) منطبق بر مراحل استاندارد بوده و به‌طور دقیق از آن پیروی می‌کند. این مورد نیز با حرف I که نشان‌دهندهٔ ابتدای کلمهٔ لاتین استاندارد است، در جدول ۴ مشخص شده است. شایان ذکر است برای پیروی از یک استاندارد، استفاده از مراحل اصلی آن برای رسیدن به هدف بسیار ضروری است. بومی‌سازی مراحل استاندارد که با علامت اختصاری FI3 در جدول نشانه‌گذاری شده است، محل تلاقی سطر دوم با عنوان مرحلهٔ اکتساب و پیاده‌سازی با بخش‌های مدیریت دارایی‌ها، مدیریت رویداد و مدیریت تداوم کسب‌وکار است. در واقع، هر یک از مدیریت‌های عنوان‌شده (دارایی، رویداد و تداوم خدمات)، در بخش پیاده‌سازی کتابخانهٔ زیرساخت فناوری اطلاعات قرار می‌گیرند. بنابراین، در کنار ایجاد تغییر در برخی مراحل، بومی‌سازی مراحل دیگر ضمن پیروی از الزامات استاندارد، موجب پیشگیری از خدشه‌دارشدن اصل این مهم می‌شود.

---

۱. مخفف FISMS به‌معنای Financial Information Security Management System یعنی سیستم مدیریت امنیت اطلاعات مالی

سطر نظارت و ارزیابی با ستون انطباق تلاقی داده شده است. این مسئله از آنجا پدید می‌آید که موضوع نظارت و ارزیابی در کتابخانهٔ زیرساخت فناوری اطلاعات با مبحث ممیزی در استاندارد، به‌طور کامل همخوانی دارد و آنچه از بررسی دقیق نتایج به‌دست می‌آید، به پیشبرد همه‌جانبهٔ فرایند ممیزی کمک شایانی می‌کند.

گفتنی است مراحلی که در آنها تلاقی میان سطرها و ستون‌ها وجود ندارد با علامت ضرب مشخص شده است.

همخوانی نقشهٔ راه ۱۱ سطحی و مدل مفهومی نمایش داده‌شده در جدول ۴، با ویژگی‌های صنعت بانکداری ایران، از جمله نکات مهمی است که به‌طور دقیق، در کانون توجه گرفته است؛ به‌گونه‌ای که ابتدا پنج رکن اصلی مرتبط با یک بانک (زارعی و جعفری نویمی‌پور، ۱۳۹۳) بدون در نظر گرفتن ایرانی یا غیرایرانی بودن آن استخراج شد؛ سپس، شاخص‌های مربوط به هر رکن که سبب تفاوت بانک‌های ایرانی و خارجی می‌شود (زارعی و جعفری نویمی‌پور، ۱۳۹۳) به شرح زیر تعیین شدند:

۱. فنی[1]: میزان دسترسی بانک‌ها به شبکهٔ وب، سرعت خطوط اینترنت در بانک‌ها، امکانات نرم‌افزاری و سخت‌افزاری موجود، پهنای باند خطوط اینترنت.
۲. فرهنگی[2]: میزان گسترش فرهنگ استفادهٔ صحیح از امکانات فناوری اطلاعات، میزان مقاومت از سوی ذی‌نفعان سیستم سنتی، میزان آشنایی مسئولان مربوطه با ساختار و عملکرد حوزهٔ امنیت فناوری اطلاعات.
۳. مدیریتی[3]: میزان جابه‌جایی و تغییر مدیران و تصمیم‌گیران، میزان ریسک‌پذیری مدیران در بهره‌مندی از سیستم‌های بانکداری الکترونیکی.
۴. مالی[4]: میزان تأمین هزینه‌های سرمایه‌گذاری در بسترهای مخابرات، میزان تأمین هزینه‌های اتصال به وب، میزان هزینه‌های توسعهٔ شبکه‌های ماهواره‌ای و رایانه‌ای، میزان تأمین هزینه‌های به‌روزرسانی شبکه‌ها.
۵. قانونی ـ حقوقی[5]: مقررات بانکداری الکترونیکی، قوانین تبادل الکترونیکی.

در نهایت بر اساس اینکه شاخص‌های بالا در سه حوزهٔ سیاست‌گذاری، اجرایی و نظارتی قرار می‌گیرد، سطوح نقشهٔ راه مدل با این رویکرد، طراحی شد.

---

1. Technological
2. Cultural-Social
3. Managerial
4. Economical- financial
5. Legal-Judicial

روش‌شناسی پژوهش

چنانچه این پژوهش را یک بررسی نظام‌یافته، کنترل شده و تجربی دربارهٔ مدیریت امنیت فناوری اطلاعات بانک‌ها بدانیم که روابط احتمالی ساختاری و سازمانی در آن، از طریق نظریه و فرضیه هدایت می‌شود، می‌توان سه دیدگاه کلی توصیف، کشف و تبیین را مدنظر قرار داد.

در ادامه مراحل اجرای پژوهش تشریح می‌شود. ابتدا به توصیف وضعیت فعلی حوزهٔ فناوری اطلاعات بانک‌ها پرداخته شد؛ سپس، طراحی و اجرای یک مدل مشخص برای پیاده‌سازی مدیریت امنیت صورت پذیرفت. در نهایت پس از اجرای مدل، دوباره تأثیر آن بر موقعیت مسئله، توصیف گردید. این پژوهش بر دیدگاه اکتشافی(ایزاک،۱۹۹۷) بنا شده است. هدف اصلی در رویکرد اکتشافی، شناخت وضعیتی است که دربارهٔ آن آگاهی‌های لازم وجود ندارد. به بیان دیگر، محقق به‌دنبال دستیابی به اطلاعاتی است که به‌کمک آنها می‌تواند موضوع تحقیق را به‌خوبی بشناسد. بنابراین با این تعریف، هدف تنها به‌دست‌آوردن برآوردی از یک مسئلهٔ خاص است (تومال، ۲۰۱۰).

این پژوهش به‌صورت کیفی و مبتنی بر روش اقدام‌پژوهی اجرا شده است که با توجه به مراحل اقدام‌پژوهی(آهنچیان و آقایی، ۲۰۱۳)، می‌توان مدل را به‌صورت زیر تعریف کرد:

الف) قرار گرفتن در شرایط مبهم قبل از پیاده‌سازی مدل؛ ناآگاهی کارکنان از اهمیت مقولهٔ امنیت، بی‌علاقگی کارکنان به درک موضوع و مشارکت در آن، کلی‌بودن قوانین سیستم مدیریت امنیت اطلاعات، نبود دستورالعمل‌های منحصربه‌فرد مدیریت امنیت اطلاعات در سیستم بانکی، نبود نقشهٔ راه معین با ذکر مراحل به‌صورت گام به گام.

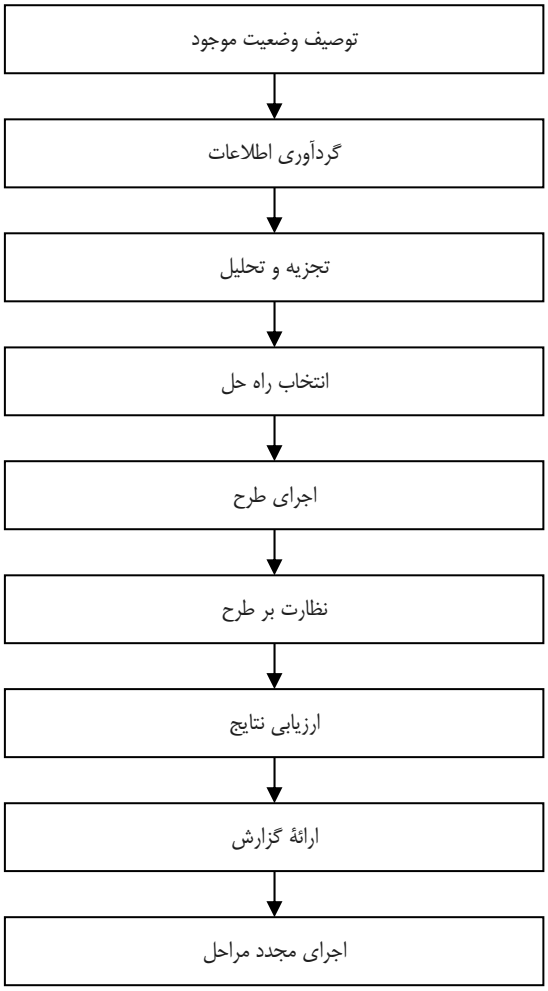
ب) برنامه‌ریزی برای چگونگی تعریف مدل؛ شناخت شرایط فعلی بانک‌ها، بررسی شرح وظایف عمومی و تخصصی واحدها، طبقه‌بندی بخش‌ها، تعیین فرایندها، مشخص کردن مسئول هر فرایند، بازنویسی مراحل مدیریت امنیت بر اساس عملکرد هر بخش و انطباق آن با استاندارد ایزو ۲۷۰۰۱، تهیهٔ فرم‌های مرتبط و تدوین دستورالعمل‌ها.

ج) اجرای مدل؛ آگاهی‌رسانی به واحدها در راستای شناخت مفاهیم مدیریت امنیت اطلاعات، تفکیک واحدها با در نظر گرفتن یک صاحب فرایند در هر واحد، ارائهٔ دستورالعمل‌ها و فرم‌های مدیریت امنیت اطلاعات به واحدها برای تکمیل، آموزشِ گام به گام اجرای مراحل هر فرایند به کارکنان، ارائهٔ برنامهٔ زمان‌بندی و اهداف مد نظر به واحدها و دریافت نتایج).

د) ارزیابی مدل؛ بازبینی مراحل انجام کار، انطباق نتایج با الزامات استاندارد، بررسی اثربخشی فعالیت‌ها در راستای هدف مدیریت امنیت اطلاعات بر اساس مدل ارائه‌شده از طریق دریافت بازخوردهاو انجام ممیزی داخلی).

ه) اصلاح دستورالعمل‌های مدل؛ بررسی مراحل ناموفق، اصلاح ساختارهای ارائه‌شده، تشخیص راه حل‌های جدید و برنامه‌ریزی برای اجرای این راه حل‌ها و بازبینی مراحل ممیزی به‌منظور انطباق با الزامات پس از انجام اصلاحات.

شمای کلی از روش اقدام‌پژوهی در این مقاله در قالب شکل ۳ به نمایش گذاشته شده است.

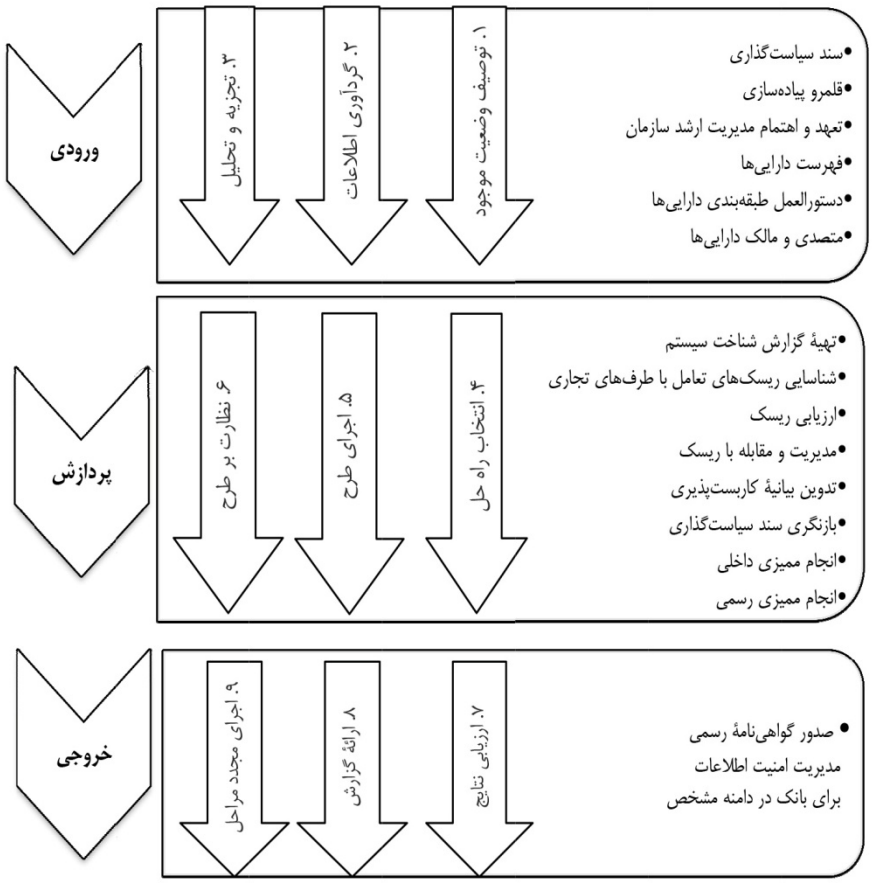


شکل ۳. چرخهٔ اقدام پژوهی در مدل مد نظر این پژوهش

منبع: مرکز نوآوری آموزشی[1] (۲۰۱۶)

1. Center for Education Innovation

ورودی‌ها، پردازش‌ها و خروجی‌های این مدل بر اساس چرخهٔ اقدام‌پژوهی به شـرح شـکل ۴ است.



شکل ٤. تعیین ورودی، پردازش و خروجی در مدل ارائه‌شده بر اساس مراحل اقدام پژوهی[1]

جامعهٔ آماری پژوهش

در این پژوهش، پس از مشخص‌کردن مدل پیاده‌سازی، بیان دستورالعمل‌ها و تـدوین فـرم‌هـای لازم، جامعهٔ آماری متشکل از ۳۷ نفر برحسب جدول ۵ به‌منظور اجرای مدل انتخاب شد.

---

۱. این شکل در بخش ورودی، پردازش و خروجی بر اساس مراحل نمودار نقشهٔ راه مدل مفهومی و در بخش پیکان‌های عمودی بـر اسـاس مراحل اقدام پژوهی به‌تصویرکشیده شده است.

جدول ۵. جامعهٔ آماری پژوهش

ردیف	موضوع	توضیحات
۱	تعداد عناصر جامعهٔ آماری	۳۷ نفر
۲	نوع طبقه‌بندی	دسته‌بندی جامعه به دو دستهٔ کارمند و مدیر (۷ مدیر و ۳۰ کارمند)
۳	تحصیلات جامعه	کارشناس و کارشناس ارشد (۱۰ کارشناس ارشد و ۲۷ کارشناس)
۴	ترکیب انسانی	۳ خانم و ۳۴ آقا
۵	ترکیب شغلی	مدیر ارشد، مدیر میانی، مدیر اجرایی،کارشناس، کاربر
۶	مقیاس پاسخ در پرسشنامه	بسیار کم، کم، متوسط، زیاد، بسیار زیاد

سپس با توجه به نوع و ترکیب جامعهٔ آماری و پیاده‌سازی مدل به‌منظور ارزیابی پژوهش و نیز دریافت نظر پرسش‌شوندگان، سؤال‌های پرسشنامه تدوین شد.

یافته‌های پژوهش

یکی از مراحل شاخص برای رسیدن به یافته‌های پیاده‌سازی سامانهٔ مدیریت امنیت اطلاعات که در سطح ۹ در بخش مدل مفهومی به آن اشاره شده است، بیانیهٔ کاربست‌پذیری است. بیانیهٔ کاربست‌پذیری، جمع‌بندی‌ای از تصمیمات اتخاذ شده در خصوص برطرف‌سازی مخاطرات، ارائه می‌دهد. این بیانیه، سند مرجع و مهمی است که کاربرد هر یک از کنترل‌های امنیتی و نحوهٔ پیاده‌سازی آن در سازمان را توضیح می‌دهد. همچنین می‌توان گفت این بیانیه، بررسی می‌کند که هیچ کنترلی، به‌طور سهوی از قلم نیفتاده باشد. در واقع با تدوین بیانیهٔ کاربست‌پذیری، راهی برای آغاز فعالیت‌های مؤثر در زمینهٔ برقراری و حفاظت از امنیت اطلاعات باز می‌شود. این بیانیه می‌تواند به‌عنوان یک سند خط‌مشی سطح بالا به‌کارگرفته شود و همچنین مبنایی برای ممیزی داخلی یا توافقنامه‌های سطح خدمات (SLA)[1] با واحدهای دیگر یا پیمانکاران بانک باشد. البته بدون این بیانیه نیز می‌توان به فعالیت‌های امن‌سازی پرداخت، اما باید توجه داشت که در این حالت نمی‌توان تداوم و کارایی مدل پیاده‌سازی را تضمین کرد.

پس از تدوین این بیانیه، باید دستورالعمل‌ها و رویه‌های اجرایی برای پیاده‌سازی روش‌های کنترلی انتخاب‌شده، بر اساس اولویت‌های سازمانی آماده و برای ابلاغ به واحدهای بانک ارسال شود. این کار را می‌توان به‌تدریج و بر اساس بودجه‌بندی و برنامه‌ریزی مناسب و با توجه به محدودیت‌های بانک انجام داد. توجه شود که ممکن است بر اساس نتایج به‌دست‌آمده از ارزیابی

1. Service Level Agreement

ریسک یا طبق سیاست‌گذاری‌های بانک، اجرای برخی روش‌های کنترلی عام ضروری تشخیص داده نشده و از فهرست روش‌های مندرج در بیانیهٔ کاربست‌پذیری اختصاصی حذف شود. این کار مانعی ندارد، اما تصویب‌کنندهٔ بیانیهٔ کاربست‌پذیری اختصاصی بانک، باید توجیه‌های لازم و کافی را در خصوص این کار داشته باشد و هنگام ممیزی آن را در اختیار ممیزان قرار دهد. اصولاً فعالیت‌های ممیزی بر اساس بیانیهٔ کاربست‌پذیری اختصاصی انجام می‌شود و در صورت عدم ارائهٔ دستورالعمل‌های اجرایی انتخاب‌شده برای حفاظت از امنیت دارایی‌های اطلاعاتی، ممکن است از صدور گواهی‌نامهٔ استاندارد خودداری شود.

نتیجه‌گیری و پیشنهادها

نتایج این پژوهش نشان می‌دهد وجود استانداردهای گوناگون مدیریت امنیت در جهان و ملزم‌کردن سازمان‌ها و نهادهای داخلی به اجرای آن، هرچند به‌صورت نمادین امکان‌پذیر است، پیاده‌سازی و اجرایی‌کردن واقعی دستورالعمل‌های مندرج در آن، باید در قالب مدل معینی در اختیار سازمان‌ها قرار گیرد. مدل ارائه‌شده در این مقاله که شامل نقشهٔ راه و دستورالعمل‌های مشخص است، از طریق بررسی دقیقِ شرایط، بومی‌سازی مراحل استاندارد ایزو ۲۷۰۰۱ و مطابقت دادن نکات مورد نیاز در حوزهٔ امنیت اطلاعات با روش‌های اجرای فرایندها در صنعت بانکداری ایران، به‌دست آمده است. بر این اساس، یک نقشهٔ ۱۱ سطحی با در نظر گرفتن اصول استاندارد مدیریت امنیت اطلاعات و نیز با تمرکز بر ویژگی‌های مؤسسه‌های بانکی ایران پیشنهاد شد. در این پژوهش حوزهٔ فناوری اطلاعات برای دامنهٔ پیاده‌سازی مدل مد نظر قرار گرفت، به همین دلیل از انطباق کتابخانهٔ زیرساخت فناوری اطلاعات و کوبیت با مراحل استقرار مدل بهره برده شد. در این خصوص چنانچه مدل کارا نباشد، ناهمخوانی آن با الزامات موجود در استاندارد به‌سرعت نمایان می‌شود و بر اساس نوع مشکل، باید روش مد نظر دوباره از مرحلهٔ نخست، بازبینی شود که در این مدل هیچ‌گونه ناهمخوانی کلی[1] یا جزئی[2] مشاهده نشد.

یکی از چالش‌های موجود در این پژوهش، طولانی‌بودن مراحل اجرای کتابخانهٔ زیرساخت فناوری اطلاعات و دشواری نحوهٔ سازگاری آن با مراحل استاندارد بود. در این خصوص یکی دیگر از نتایج مهم استفاده از این مدل، شکل‌گیری جدول متقاطع مفهومی از نحوهٔ تقابل مراحل کتابخانهٔ زیرساخت فناوری اطلاعات و کوبیت با شرایط استقرار مراحل فرایند استاندارد است. این

1. Major
2. Minor

جدول سبب می‌شود که هر دو بخش زیرساخت و الزامات، بدون وجود مشکلاتی از قبیل تکراری بودن مباحث یا ناسازگاری مراحل با یکدیگر (آماده و جعفرپور، ۲۰۱۰)، پیاده‌سازی شوند.

منابع

آهنچیان، م. و آقایی، م. م. (۱۳۹۴). *اقدام پژوهی از طراحی تا ارزیابی*. تهران: انتشارات رشد.

ایزاک، ا.؛ ترجمه دلاوری. (۱۳۷۶). *راهنمای تحقیق و بررسی*. تهران: انتشارات ارسباران.

تاج‌فر، ا. ه.؛ محمودی میمند، م.؛ رضا سلطانی، ف. و رضا سلطانی، پ. (۱۳۹۳). رتبه‌بندی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف. *نشریهٔ مدیریت فناوری اطلاعات*، ۶(۴)، ۵۶۶- ۵۵۱.

جراحی، م.؛ عظیمی، ع. و جراحی، ع. (۱۳۸۷). پیاده‌سازی امنیت اطلاعات در بانک‌ها. *پنجمین کنفرانس بین‌المللی مدیریت فناوری اطلاعات و ارتباطات*. تهران، ۳۰-۲۹ بهمن.

شالی، ع. (۱۳۸۴). مدیریت سیستم‌های امنیت اطلاعات. *مجلهٔ الکترونیکی مرکز اطلاعات و مدارک علمی ایران*، ۴(۴)، ۳-۲.

موسوی، پ.؛ یوسفی زنوز، ر. و حسن‌پور، ا. (۱۳۹۴). شناسایی ریسک‌های امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری، *نشریهٔ مدیریت فناوری اطلاعات*، ۷(۱)، ۱۸۴- ۱۶۳.

نادری خورشیدی، ع. و قاسمی نژاد، ی. (۱۳۹۳). بررسی شاخص‌های تأثیرگذار بر موفقیت راهکارهای خدمات بانکداری نوین از دید مدیران و نخبگان بانک انصار. *نشریهٔ مدیریت فناوری اطلاعات*، ۶ (۳)، ۵۰۴- ۴۸۷.

وثوق، م.؛ تقوی فرد، م. ت. و البرزی، م. (۱۳۹۳). شناسایی تقلب در کارت‌های بانکی با استفاده از شبکهٔ عصبی مصنوعی، *نشریهٔ مدیریت فناوری اطلاعات*، ۶(۴)، ۷۴۶-۷۲۱.

Abbasi, P., Rajkamal, I., Jose luis, P. & Francese, R. (2016). Securities trading by banks and credit supply: micro evidence from the crisis. *Journal of Financial Economics Elsevier,* 121(3), 569–594.

Ahanchian, M. & Aghaee, M. (2013). Action research from design to assessment. *Tehran: Roshd*. (*in Persian*)

Amadeh, H. & Jafar Pour, M. (2010). Barriers and strategies for the development of electronic banking. *Journal of Executive Mangement*.

Brain, F. (2007). Banks claim share of credit card security cost is unfair. *Computer world, 41* (26), 14-19.

Brenner, J. (2007). ISO 27001: Risk management and compliance. *Risk Management, 54* (1), 24-30.

Bruno Britz, M. (2006). Corillian maps to ISO security standard companys certification to ISO 27001 standard to provide greater assurance to clients. *Bank system & technology, 43* (8), 19-21.

Coa, J. & Song, W. (2016). Risk assessment of co creating value with costumers: a rough group analytic network process approach. *Expert system with applications, 55* (15), 145-156.

Colin, W. (2000). Security is an essential ingredient. *The banker,* 150 (896), 132.

Green Meier, L. (2006). Follow the ISO path to security. *Information week* , 30(5), 69-70.

Hinson, G. (2007). The state of IT auditing in 2007. *Taylor & Francis* ,10(2), 13-31.

Isac, E. (1997). *Research and investigation guide.* Trans by Delavari, Tehran: Arasbaran. (*in Persian*)

Jarahi, M., Azimi, A. & Jarahi, A. R. (2000). Implementing information security in banks. *Fifth International Conference on Information and Communication Technology Management*, Tehran,17-18 Feb. (*in Persian*)

Karyda, M., Tsohou, A. & Kokolakis, S. (2015). Analyzing the role of cognitive and cultutal biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & security, 52*(3), 128-141.

Miller, S. (2016). Enterprise risk management, a common framework for the entire organization. *procedia economics and finance Elsevier*, 5(6), 141-149.

Modiri, N., Sheikhpour, R. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. *Indian journal of science and technology, 5*(2), 70.

Moosavi, P., Zonooz, R. Y. & Hasanpour, A. (2015). Identify organizational information security risks in the banking industry using fuzzy Delphi. *IT Management* ,7 (1) 163-184. (*in Persian*)

Naderi khoorshidi, A. R. & Ghasemi Nezhad, Y. (2014). Check indicators affecting the success of an online banking solutions from the perspective of managers and elite Ansar Bank. *IT Management*, 6(3), 487-504. (*in Persian*)

Ostrowska, M. & Mazur, S. (2015). Risk in crisis situation. *procedia economics and finance Elsevier*, 23(10), 615-621.

Shali, A. A. (2005). Information security management systems. *Electronic Journal of Information and Documentation Center of Iran*, 4(4), 2-3. (*in Persian*)

Streff, K., & Rajagopalan, A. (2006). Adaptive bank transaction camouflaging system. *ABC*, 15(7), 10-12.

Tajfar, A. H., Meymand, M. M., Reza Soltani, F. & Reza Soltani, P. (2015). Ranking barriers to implementing information security management system and assess preparedness of exploration management. *IT Management*, 6(4), 551-566. (*in Persian*)

Tomal, D. (2010). Action research for educators. *Rowman & little field education*, 2 (20), 200-202.

Violino, B. (2006). Sorting The Standards. *Computerworld*, 5(3), 40-46.

Vosugh, M., Taghavi Fard, M. T. & Alborzi, M. (2014). Bank card fraud detection using artificial neural network. *IT Mangement*, 6(4), 721-746. (*in Persian*)

Wolden, M., Valverde, R. & Talla, M. (2015). The effectiveness of CObIT5 in information security framework for reducing cyber attacks on supply chain management system. *IFAC papers online*, 48(3), 3-48.