INSO-ISO-IEC-TR

27016

1st. Edition

2015
Identical with
ISO/IEC TR 27016:
2014

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standards Organization

استاندارد ملی ایران – ایزو – آی ای سی – تی آر
۲۷۰۱۶
چاپ اول
۱۳۹۳

فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- اقتصادهای سازمانی

Information technology — Security techniques — Information security management — Organizational economics

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- اقتصادهای سازمانی »

رئیس :	**سمت و/ یا نمایندگی**
ایزدپناه، سحرالسادات (فوق لیسانس مهندسی فناوری اطلاعات)	کارشناس مسؤول سازمان فناوری اطلاعات ایران
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر نرم‌افزار، فوق لیسانس مدیریت اجرایی)	مدیرکل سازمان فناوری اطلاعات ایران
اعضاء : (اسامی به ترتیب حروف الفبا)	
بخشایش، سعید (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت فناوران توسعه امن ناجی
آریا، بهناز (دکتری مهندسی کامپیوتر)	قائم مقام مؤسسه کهکشان نور
سجادیه، علیرضا (فوق لیسانس مهندسی کامپیوتر)	مدیرعامل شرکت پردازشگران
طی نیا، رضا (فوق لیسانس مدیریت فناوری اطلاعات)	مدیر عامل شرکت کاربرد سیستم
قسمتی، سیمین (فوق لیسانس فناوری اطلاعات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
جمیل‌پناه، ناصر (فوق لیسانس کامپیوتر)	کارشناس ارشد حوزه مخابرات
مغانی، مهدی (فوق لیسانس ریاضی کاربردی)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات
ناظمی، اسلام (دکترای مهندسی کامپیوتر نرم‌افزار)	استادیار دانشگاه شهید بهشتی
نصیری آسایش، حمید رضا (فوق لیسانس فناوری اطلاعات معماری سازمانی)	پژوهش‌گر دانشگاه شهید بهشتی

یعقوبی رفیع، کمال‌الدین پژوهش‌گر دانشگاه شهید بهشتی
(فوق لیسانس فناوری اطلاعات معماری سازمانی)

فهرست مندرجات

عنوان **صفحه**

کمیسیون فنی تدوین استاندارد ج
پیش‌گفتار و
۱ هدف و دامنه کاربرد ۱
۲ مراجع الزامی ۱
۳ اصطلاحات وتعاریف ۱
۴ کوته‌نوشت‌ها ۴
۵ ساختار این استاندارد ۵
۶ عوامل اقتصادی امنیت اطلاعات ۵
۶-۱ تصمیمات مدیریت ۵
۶-۲ موردهای کسب‌وکار ۶
۶-۳ سهام ذی‌نفعان ۹
۶-۴ بازنگری تصمیم اقتصادی ۱۰
۷ اهداف اقتصادی ۱۰
۷-۱ مقدمه ۱۱
۷-۲ ارزش‌گذاری نسبت به تغییر دارایی‌های اطلاعاتی ۱۱
۸ تراز نمودن اقتصاد امنیت اطلاعات برای ISM ۱۴
۸-۱ مقدمه ۱۴
۸-۲ منافع اقتصادی ۱۴
۸-۳ هزینه‌های اقتصادی ۱۵
۸-۴ کاربرد محاسبات اقتصادی برای ISM ۱۶
۸-۴-۱مرور کلی ۱۶
۸-۴-۲راهنما ۱۷
۸-۴-۳یک مورد کسب‌وکار مبتنی بر رویکرد کل سازمان (رده الف) ۱۹
۸-۴-۴یک مورد کسب‌وکار مبتنی بر یک بخش سازمان (رده ب) ۲۰
پیوست الف(اطلاعاتی)شناسایی ذی‌نفعان و هدف‌ها برای تنظیم ارزش‌ها ۲۲
پیوست ب(اطلاعاتی)تصمیمات اقتصادی و عوامل اصلی هزینه تصمیم‌گیری ۲۴
پیوست پ(اطلاعاتی) مدل‌های اقتصادی مناسب برای امنیت اطلاعات ۳۱
پیوست ت(اطلاعاتی)مثال‌های محاسبه موارد کسب‌وکار ۳۶
کتاب‌نامه ۴۲

پیش‌گفتار

استاندارد « فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- اقتصادهای سازمانی » که پیش‌نویس آن در کمیسیون‌های مربوط توسط سازمان فناوری اطلاعات ایران تهیه و تدوین شده است و در سیصد و شصت و دومین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۳/۱۱/۲۹ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران ، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع ، علوم و خدمات ، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود ، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین ، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

منبع و مآخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC TR 27016: 2014, Information Technology — Security Techniques — Information Security Management — Organizational Economics

فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- اقتصادهای سازمانی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین راهنماهایی درباره نحوه تصمیم‌گیری سازمان به‌منظور حفاظت اطلاعات و شناسایی پیامدهای اقتصادی این تصمیمات در زمینه الزامات رقابتی برای منابع است.

این استاندارد برای همه سازمان‌ها با هر نوع و اندازه کاربردپذیر است و اطلاعاتی برای سازمان‌ها فراهم می‌آورد تا مدیریت ارشد که مسئولیت تصمیمات امنیت اطلاعات را به عهده دارد بتواند، تصمیمات اقتصادی در مدیریت امنیت اطلاعات را اتخاذ نماید.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد محسوب می‌شوند.

درصورتی‌که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مرجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*[1]

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف تعیین‌شده در ISO/IEC 27000، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود:

۳-۱

انتظار زیان سالیانه(ALE)[2]

زیان (به بند ۳-۱۳ مراجعه شود) سالیانه برای یک دارایی که به دلیل مخاطره در طول یک دوره یک‌ساله می‌توان انتظار داشت.

یادآوری- ALE به این‌صورت تعریف می‌شود: ALE = SLE * ARO که در آن SLE، انتظار زیان مقطعی[3] و ARO، نرخ وقوع سالیانه[4] است.

---

۱ - استاندارد بین‌المللی ISO/IEC 27000 در سال ۱۳۹۱ با شماره ملی ۲۷۰۰۰ منتشر شده است.

2 - Annualized loss expectancy

3 - Single Loss Expectancy

4 - Annualized Rate of Occurrence

۲-۳

ارزش مستقیم[1]

ارزشی که می‌توان، در صورت وقوع آسیب یا از بین رفتن دارایی اطلاعاتی یا دارایی‌ها، از طریق ارزش جابه-جایی یا جایگزینی مشابه تعیین نمود.

یادآوری- این ارزش تا زمانی‌که دارایی اطلاعاتی دستخوش آسیب نشده باشد، مثبت است، در صورتی زیان محسوب می‌شود که رویدادی رخ دهد.

۳-۳

عامل اقتصادی[2]

اقلام یا اطلاعاتی که بر ارزش دارایی اثر می‌گذارد (به بند ۳-۲۲ مراجعه شود)

۴-۳

مقایسه اقتصادی[3]

پرداختن به موارد رقابتی یا جایگزین جهت تخصیص منابع است.

۵-۳

توجیه اقتصادی[4]

عنصری از مورد کسب‌وکار که برای امکان تخصیص منابع طراحی شده است.

۶-۳

ارزش افزوده اقتصادی[5]

سنجه‌ای که سود بهره‌برداری (سود عملیاتی) خالص را با هزینه کل سرمایه مورد مقایسه قرار می‌دهد.

۷-۳

علم اقتصاد[6]

استفاده کارامد از منابع محدود است.

۸-۳

ارزش مورد انتظار[7]

ارزش برآوردشده به‌عنوان یک عامل موثر بر کار به‌وسیله دارایی‌های اطلاعاتی آسیب دیده یا ازدست‌رفته است.

یادآوری- این ارزش تا زمانی‌که دارایی اطلاعاتی دستخوش آسیب نشده مثبت است، در صورتی زیان محسوب می‌شود که رویدادی رخ دهد.

۹-۳

ارزش توسعه یافته[8]

ارزش مورد انتظاری که میزان ارزش را چند برابر می‌کند.

1- Direct value
2- Economic factor
3- Economic comparison
4- Economic justification
5- Economic value added
6- Economics
7- Expected value
8- Extended value

۱۰-۳

ارزش غیرمستقیم[1]

ارزشی که در صورت رویداد آسیب یا ضرر دارایی‌های اطلاعاتی یا دارایی‌ها، برای جایگزینی یا بازسازی تخمین زده می‌شود.

یادآوری- این ارزش تا زمانی‌که دارایی اطلاعاتی دستخوش آسیب نشده باشد، مثبت است، در صورتی منفی محسوب می‌شود که رویدادی رخ دهد.

۱۱-۳

اقتصاد امنیت اطلاعات[2]

استفاده کارامد از منابع محدود برای مدیریت امنیت اطلاعات است.

۱۲-۳

مدیریت امنیت اطلاعات (ISM)[3]

مدیریت حفظ محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات است.

۱۳-۳

زیان[4]

کاهش ارزش (به ۳-۲۲ مراجعه شود) یک دارایی است.

یادآوری- ممکن است در چارچوب اقتصاد امنیت اطلاعات (به بند ۳-۱۱ مراجعه شود) به صورت یک مقدار مثبت به کار رود. هزینه در این اسناد و مدارک همیشه منفی است مگر غیر از این بیان شود.

۱۴-۳

ارزش بازار[5]

بالاترین قیمت حاضر و آماده که خریدار خواهد پرداخت و پایین‌ترین قیمتی که یک فروشنده قبول خواهد کرد.

۱۵-۳

خالص ارزش فعلی[6]

مجموع ارزش‌های فعلی (به بند ۳-۱۶ مراجعه شود) جریان نقدی انفرادی برای همان موجودیت است.

۱۶-۳

ارزش فعلی[7]

ارزش فعلی مجموع پول یا سرازیر شدن جریان نقدی آتی که برای یک نرخ برگشت خاص ارائه شده است.

۱۷-۳

سود غیر اقتصادی[8]

سودی که برای آن هیچ پرداختی[9] انجام نمی‌شود.

1- Indirect value
2-Information security economics
3- Information security management
4- Loss
5- Market value
6- Net present value
7- Present value
8- Non economic benefit
9- Payment

۱۸-۳
هزینه فرصت[1]

هزینه تخمین زده‌شده آتی برای فعالیت‌ها یا فعالیت امنیت اطلاعات خاص است.

۱۹-۳
ارزش فرصت[2]

ارزش مثبت تخمین زده‌شده آتی که از فعالیت‌ها یا فعالیت امنیت اطلاعات خاص به‌دست خواهد آمد.

۲۰-۳
الزامات مقرراتی[3]

تقاضای منابع واجب مربوط به یک بازار خاص است.

۲۱-۳
بازگشت سرمایه[4]

اندازه‌گیری دوره‌ای بازده مقدار سرمایه‌گذاری شده در یک موسسه اقتصادی است.

۲۲-۳
ارزش اجتماعی[5]

تمایز عمومی بین درست و غلط است.

۲۳-۳
ارزش[6]

ارزش نسبی یک دارایی نسبت به اشیاء یا یک ارزش کاملا تعریف‌شده‌ی دیگر است.

یادآوری- در اقتصاد امنیت اطلاعات (به بند ۳-۱۱ مراجعه شود) یک مقدار ممکن است مثبت یا منفی باشد. در این استاندارد مقدار همیشه مثبت است مگر آنکه غیر از آن بیان شود.

۲۴-۳
ارزش در مخاطره[7]
VAR

تجمیع بیشترین زیان (به بند ۳-۱۳ مراجعه شود) در زمان هدف که از احتمال ارائه شده فراتر نخواهد رفت.

یادآوری- زمان هدف برای مثال می‌تواند ۱ سال باشد و احتمال ارائه شده به‌عنوان سطح اطمینان در نظر گرفته می‌شود.

۴ کوته‌نوشت‌ها

BVM	Basic Value Model	مدل ارزش پایه
CIA	Confidentiality–Integrity–Availability	محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات

1- Opportunity cost
2- Opportunity value
3- Regulatory requirements
4- Return on investment
5- Societal value
6- Value
7- Value-at-risk

ICT	Information and Communications Technology	فناوری اطلاعات و ارتباطات
IRP	Interest Rate Parity	برابری نرخ بهره
ISMS	Information Security Management System	سامانه مدیریت امنیت اطلاعات
ROI	Return On Investment	بازگشت سرمایه

۵ ساختار استاندارد

قسمت اصلی علم اقتصاد سازمانی مدیریت امنیت اطلاعات، توانایی جهت ارائه ارزش‌های اقتصادی برای مدیریت است و از این طریق می‌توانند تصمیمات بهتری بر پایه واقعیت در خصوص منابع به‌کار رفته جهت حفاظت از دارایی‌های اطلاعاتی سازمان اتخاذ کنند.

در بند ۶ از این استاندارد، عوامل اقتصادی امنیت اطلاعات و تناسب آن‌ها در مدیریت تصمیم‌گیری توصیف می‌شود. بند ۷، اهداف اقتصادی را در چارچوب ارزیابی دارایی شرح می‌دهد. بند ۸، نحوه کاربرد ترازنامه اقتصادی را با استفاده از مزیت‌های امنیت اطلاعات و هزینه‌ها در زمینه[1] سازمانی به‌صورت کلی و استفاده از نمونه‌های وابسته به رده مورد کسب‌وکار بیان می‌کند.

این بندها توسط تعدادی از پیوست‌ها پشتیبانی می‌شوند:

- پیوست الف اهداف قشر وسیعی از سهامداران را در خصوص ارزش امنیت اطلاعات توصیف می‌کند.
- پیوست ب اهداف کاری و هزینه‌های سازمانی امنیت اطلاعات را توصیف می‌کند
- پیوست پ مجموعه مدل‌هایی را شرح می‌دهد که می‌توان برای علم اقتصاد سازمانی امنیت اطلاعات به کاربرد.
- پیوست ت نمونه‌هایی را با استفاده از مدل‌هایی به همراه تصاویر نمونه شرح می‌دهد.

۶ عوامل اقتصادی امنیت اطلاعات

۶-۱ تصمیمات مدیریت

مجموعه استانداردهای ISO/IEC 27000 چندین هدف مربوط به کسب‌وکار هدایت‌کننده تصمیمات مدیریت را ارائه می‌کنند که سازمان به‌وسیله آن‌ها به‌طور رسمی و غیررسمی نیازشان را به سرمایه‌گذاری در زمینه امنیت اطلاعات ارزیابی می‌کنند. این تصمیمات مدیریتی در صورتی موثرتر خواهند بود که فرایند مربوطه برای مقایسه سود خالص سرمایه‌گذاری امنیت اطلاعات همراه با تقاضاهای رقیب برای منابع در سایر بخش‌های سازمان طراحی می‌شود فرایند تصمیم‌گیری در زمینه امنیت اطلاعات نیازمند در برگرفتن یک مبنای مشخص در تایید تصمیم‌گیری مدیریت، به‌حساب آوردن عامل‌های مربوطه با توجه به علم اقتصاد امنیت اطلاعات سازمان می‌باشد. توصیه می‌شود ارزش اقتصادی سرمایه‌گذاری امنیت اطلاعات را به‌عنوان هدف کاری سازمان به‌حساب آورد. با پیوند مستقیم اهداف کاری، عوامل دیگری مانند مخاطرات، هزینه‌ها و مزایا را می‌توان برای اندازه‌گیری موثر به‌کار برد. مشخص کردن یک توجیه اقتصادی مناسب برای تخصیص منابع جهت حفظ امنیت دارایی‌های اطلاعاتی به شیوه‌ای که مقایسه اقتصادی با شیوه‌های دیگر کاربرد منابع

1- Context

امکان‌پذیر باشد نیازمند بررسی از جانب مدیریت است. اصل به‌کاربردن رویکرد تخصیص منابع (ارزش فعلی خالص، بازده سرمایه‌گذاری، ارزش‌افزوده اقتصادی) برای برنامه مدیریت امنیت اطلاعات به‌منظور تولید نتایجی است که با اهداف تصمیم‌گیری قابل‌مقایسه باشد.

الف) ممکن است بعضی از مزیت‌های برنامه مدیریت امنیت اطلاعات ذاتا جنبه اقتصادی نداشته باشد زیرا اندازه‌گیری عینی و منسجم سود در قالب اصطلاحات اقتصادی دشوار است. به‌عنوان مثال، اگر الزامات قانونی برای تایید یا تامین اطلاعات خاصی وجود داشته باشد، تعیین ارزش اقتصادی سود آن امکان‌پذیر نیست و همچنین از آن به‌عنوان ارزش تطابق[1] یاد می‌شود.

ب) به‌طور مشابه ارزش اجتماعی یک برنامه مدیریت امنیت اطلاعات را نمی‌توان به‌طور عینی در قالب اصطلاحات اقتصادی فاقد یک سازوکار بازخورد موثر از طرف جامعه تعیین کرد. سودهای غیراقتصادی بخش مهمی از توجیه برنامه مدیریت امنیت اطلاعات هستند بااین‌حال هیچ شکلی از تحلیل مالی را در بر نمی‌گیرد زیرا کاربرد آن در اندازه‌گیری ثابت دشوار است.

پ) امنیت اطلاعات را می‌توان برای حفاظت از دارایی‌های غیرملموس مانند علامت تجاری، شهرت و غیره به‌کار برد. لازم است میزان این حفاظت محاسبه‌شده و به طریقی ارائه گردد که برای ارزیابی سازمان از آن دارایی‌های نامشهود ارائه می‌گردد. توصیه می‌شود علم اقتصاد به‌کار رفته در این ارزیابی با اثر کاربرد امنیت اطلاعات برای دارایی نامشهود مرتبط باشد. ارزش‌های اقتصادی از کارکردهای تجاری همانند مدیریت مخاطره، مالی، فروش‌ها و بازاریابی و غیره منشا می‌گیرد. توصیه می‌شود هزینه‌های حفاظت را بر اساس امنیت اطلاعات محاسبه کرد.

۶-۲ موردهای کسب‌وکار

یک مورد سرمایه‌گذاری در امنیت اطلاعات به سازمان امکان می‌دهد تا بررسی کند آیا مزایای اقتصادی بر هزینه‌ها برتری دارد یا خیر و این برتری تا چه حد است. معمولا اهداف امنیت اطلاعات برای مدیریت یک سازمان به شکل مورد کسب‌وکار ارائه می‌یابد و توصیه می‌شود به جنبه‌های اقتصادی پرداخته شود. توصیه می‌شود این بررسی، عواقب ناشی از بررسی جنبه‌های امنیت اطلاعات مسئله کاری را در برگیرد. به‌عنوان مثال تاثیر اقتصادی بر توانایی سازمان جهت تامین اهداف آن در صورت انجام (عدم انجام) فعالیت چه خواهد بود؟ توصیه می‌شود هدف یک کار ارائه یک پاسخ روشن به این سوال باشد.

توصیه می‌شود مورد کسب‌وکار یک دیدگاه متعادل هزینه- منفعت- مخاطره را ارائه دهد، پس سازمان از گزینه‌ها و مفاهیم ضمنی هر تصمیم‌گیری آگاه است، بنابراین توانایی یک مبنا به همراه اشتیاق برای سرمایه‌گذاری در امنیت را می‌توان برای رسیدن به بهترین نتایج مد نظر قرارداد. این مفاهیم و گزینه‌ها در قالب سرمایه‌گذاری صحیح در زمینه امنیت اطلاعات مثبت هستند و در صورت سرمایه‌گذاری نامناسب منفی می‌شود.

توصیه می‌شود مورد کسب‌وکار در چارچوب هزینه‌های سرمایه‌گذاری برای امنیت اطلاعات در مقابل هر هزینه مربوط به مخاطرات مورد بررسی قرار گیرد. توصیه می‌شود اقلام زیر بنایی اصلی مورد کسب‌وکار

۱- Value of compliance

اطلاعات کافی برای تصمیم گیرندگان تامین کنند تا به شناخت این موارد دست یابند.

الف) ارزش دارایی اطلاعاتی

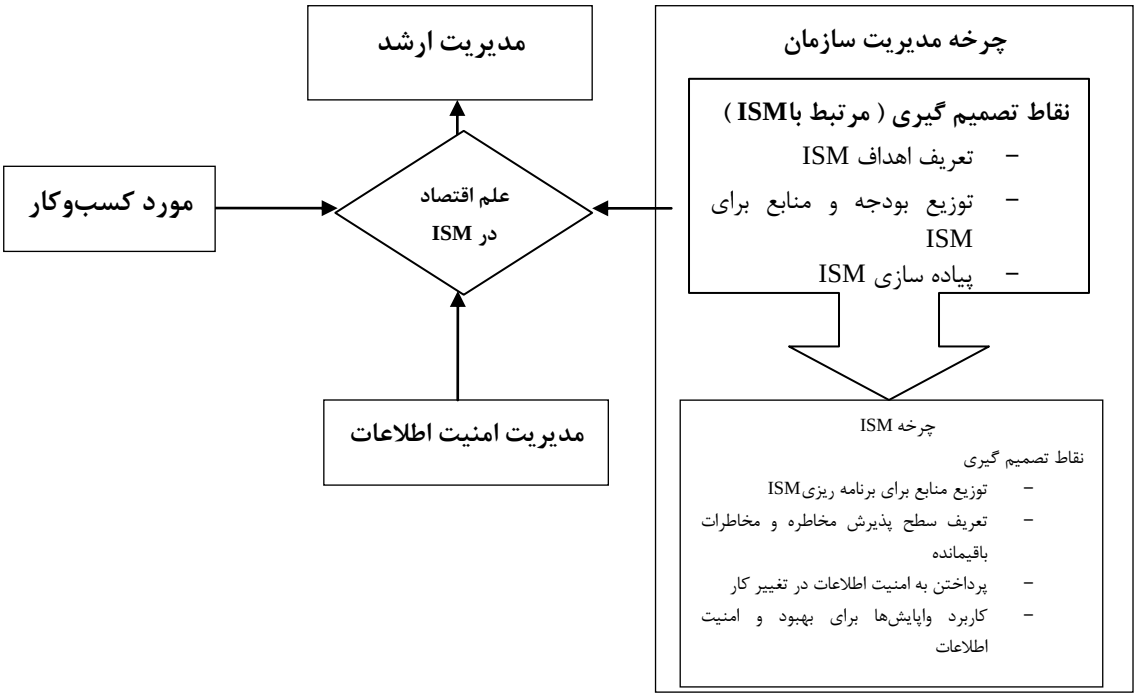
ب) مخاطرات بالقوه دارایی اطلاعاتی

پ) هزینه مشخص حفاظت از دارایی اطلاعاتی

ت) کاهش مخاطره در رابطه با محافظت

از بعضی جهات هزینه حفاظت به‌کار رفته برای ارزش دارایی اطلاعاتی به نقطه تعادل بهینه خواهد رسید. این نقطه بهینه زمانی در هزینه‌های حفاظت قرار می‌گیرد که کاهش مخاطره موثر بر ارزش کمتر از هزینه حفاظتی باشد (به بند پ-۳ مراجعه شود).

شکل ۱ مورد کسب‌وکار در بردارنده عوامل اقتصادی را به‌عنوان بخشی از فرایند کار به‌صورت نماد نشان می‌دهد.



شکل 1- فرایند تصمیمات اقتصادی سازمانی در رابطه با امنیت اطلاعات با استفاده از استاندارد ۲۷۰۱۶

زمانی که آماده‌سازی یک مورد کسب‌وکار نیاز باشد لازم است سازمان مراقب باشد زیرا منابع همیشه محدود بوده و لازم است بخش‌های حساس بسته به نیازهای سازمان مورد بررسی قرار گیرد. توصیه می‌شود جنبه‌های امنیت اطلاعات را در این زمینه بر مبنای حقایق و اطلاعات قطعی پایه‌گذاری شود در این صورت توصیه می‌شود، محاسبات بر مبنای بهترین دانش و تجربه انجام شود، که ممکن است دربرگیرنده موارد زیر باشد.

ث) محاسبه با یک بازه زمانی (بیشینه، کمینه دوره زمانی، غیره).

ج) تخمین هزینه‌ها

چ) نقل قول‌ها

ح) پیش‌بینی ارزش‌های بازار
خ) جرایم و کارمزدهای غیرقابل انطباق یا شناسایی‌شده
د) پیامدهای قانونی در تعاریف اقتصادی مستقیم و یا غیرمستقیم
ذ) برآورد مخاطره که پیش‌بینی‌هایی از ضررهای در حال وقوع ارائه می‌دهد
ر) ارزش فرصت
ز) هزینه فرصت

وقتی برآوردها بر اساس بازه زمانی انجام می‌گیرد، می‌توان این‌ها را از آمار، ارزیابی مخاطره و غیره جمع‌آوری کرد. هنگام تعریف یک بازه، مشورت کردن با متخصصان درباره همه عملکردها و فضاهای مربوطه مفید است.

توصیه می‌شود علم اقتصاد در ارتباط با مدیریت امنیت اطلاعات جنبه‌های زیر را پوشش دهد:

ز) فعالیت‌ها و تصمیمات در طول فرایند مدیریت امنیت اطلاعات
س) جنبه‌های اقتصادی تایید کننده تصمیم‌گیری در سرمایه‌گذاری‌های سالانه برای فرایند مدیریت امنیت اطلاعات
ش) اطمینان از پذیرفته شدن مدیریت امنیت اطلاعات در تطابق با استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷(سامانه مدیریت امنیت اطلاعات)

پیچیدگی مورد کسب‌وکار برای مدیریت امنیت اطلاعات به دامنه کاربردی بستگی دارد و بر اساس محتوایی است که امنیت اطلاعات باید در آن به‌کار برده شود. به‌منظور گنجاندن اقتصاد سازمانی امنیت اطلاعات به‌عنوان بخشی از مورد کسب‌وکار، لازم است یک اصل منطقی تجاری مبتنی بر توصیف تجاری همراه با راه‌حل واقعی امنیت اطلاعات سنجیده شود. روش‌های اقتصادی متفاوتی را می‌توان برای یک مورد کسب‌وکار در سطوح متفاوت سازمان به‌کار برد. این سطوح می‌توانند به‌سادگی استفاده از دو رده باشند : رده الف – تمام سازمان و رده ب – بخشی از سازمان که از یک فرایند، کارکرد و غیره تشکیل شده است. بخش سازمانی می‌تواند تعدادی از دارایی‌ها را شامل شود. رده ب از دیدگاه مدیریت امنیت اطلاعات می‌تواند یک کاربرد مورد کسب‌وکار برای واپایش یا واپایش‌ها باشد.

جدول ۱- رده‌بندی موارد کسب‌وکار

رده مورد کسب-وکار	نوع / دامنه کاربرد	توصیف نوع مورد کسب‌وکار	نمونهISM	ویژگی‌های محاسبه
الف	تمام سازمان	سطح بالا و بسیار مفهومی به این معنی که مورد امنیت اطلاعات به‌کار رفته برای کل یا بخش اصلی سازمان را توصیف می‌کند	یک نمونه موردی برای اجرای ISMS، ادغام یا کسب یک سازمان دیگر است. فرض می‌شود ISMS گستره سازمان برای مرزهای دامنه کاربرد مورد توافق به‌کار می‌رود	محاسبه سطح بالای ارزش‌های فرصت برای سازمان و هزینه‌ها برای پیاده‌سازی و اجرای مورد کسب‌وکار. یک محدوده برای ارزش‌ها و هزینه‌ها پیشنهاد می‌شود.
ب	بخشی از سازمان مانند فرایند / واحد / کارکرد / یا دارایی / دارایی‌ها و / یا واپایش / واپایش	یک مورد مبتنی بر یک فعالیت تجاری یا یک فعالیت امنیت اطلاعات. این مورد تغییر را به‌عنوان بخشی از کار مد نظر قرار داده و امنیت اطلاعات به‌کار رفته برای تغییر و سرمایه‌گذاری برای سازمان را با تأثیرات چندگانه بر امنیت اطلاعات توصیف می‌کند این مورد امنیت اطلاعات به‌کار رفته برای یک دارایی خاص یا مجموعه‌ای از دارایی‌ها را توصیف می‌کند در این صورت توصیه می‌شود چندین واپایش به‌کار برده شود.	نمونه مورد یک برون‌سپاری ICT، مرکز رایانه و یا اقلامی همانند وب امن، افزایش حفاظت پیرامون ، حفاظت مرکز رایانه آتش، آماده‌سازی IDS و غیره.	چندین محاسبه می‌تواند وجود داشته باشد و ممکن است تجمیع نتایج ضروری باشد. تعیین محاسبه ارزش‌ها و هزینه‌ها به‌طورکلی آسان است اما ممکن است برای موردهای کسب‌وکار پیچیده برآورد شود. یک محدوده فقط برای برآوردهای ارزش‌ها پیشنهاد می‌گردد اما برای هزینه‌ها پیشنهاد نمی‌گردد.

اطلاعات بیشتر درباره تصمیمات اقتصادی و عامل‌های اصلی تصمیم‌گیری در پیوست ب توصیف می‌شوند.

۳-۶ سهام ذی‌نفعان

استاندارد ملی ایران به شماره ۲۷۰۰۱: سال ۱۳۸۷ تصریح می‌کند که توصیه می‌شود ISMS را برای کمک به سهام ذی‌نفعان به‌کار برد. توصیه می‌شود کمک به پیش برد سهام ذی‌نفعان، پرداختن به اقتصاد امنیت اطلاعات را در بر گیرد. توصیه می‌شود عوامل اقتصادی در جایی که امنیت اطلاعات می‌تواند تاثیر منفی بر ذی‌نفعان داشته باشد مدنظر قرار گیرد. به‌عنوان مثال ارزش‌های زیر را می‌توان به‌کار برد:

الف) ارزش اجتماعی، به‌عنوان مثال، آیا توصیه می‌شود کل ارزش اقتصادی جامعه تعریف‌شده در برگرفته شود یا توصیه می‌شود محدودیت‌هایی وجود داشته باشد؟
ب) ارزش علامت تجاری، ارزش اصلی تجارت و غیره
پ) شهرت
ت) ارزش مشتری
ث) IPR (حقوق مالکیت معنوی)
ج) ممکن است ارزش‌های اقتصادی خاصی بسته به نوع کار مانند بخش بهداشت و سلامت، بخش حمل‌ونقل و غیره مورد نیاز باشد.
احتمال دارد سایر کارکردهای یک سازمان این ارزش‌ها را از پیش برای محاسبات اقتصادی‌شان مد نظر قرار دهند و توصیه می‌شود برای تامین ورودی باارزش در هنگام پرداختن به امنیت اطلاعات تشویق شوند.
برای اطلاعات بیشتر درباره ذی‌نفعان و اهداف آن‌ها به پیوست الف مراجعه شود.

۴-۶ بازنگری تصمیم اقتصادی

اجرا و مدیریت در جریان واپایش‌های امنیت اطلاعات برای حفاظت از دارایی‌های اطلاعاتی، منابع سازمانی محدود را مصرف خواهد کرد. بنابراین توصیه می‌شود به‌عنوان یک قلم از ارزش به همراه انتظار بازدهی یک بازده مطلوب در آینده (مثل جلوگیری از سرقت اطلاعات حساس) توسط سازمان با آن‌ها رفتار شود.
همان‌طور که در استاندارد ISO/IEC 27004 توصیف شد، یک سازمان به‌طور پیوسته به ارزیابی و اندازه‌گیری نیاز دارد که آیا امنیت اطلاعات به‌کار رفته به هدف موردنظر خودش خواهد رسید یا خیر. این فرایند سنجش نیز برای ارزیابی سرمایه‌گذاری اقتصادی انجام‌شده توسط سازمان در کالاها و خدمات مجدد به‌کار می‌رود. به‌عنوان مثال، هزینه‌های فعالیت‌های زیر منطقی هستند :
الف) هزینه فرآیندها و پروژه‌های ارزیابی مخاطره.
ب) زیرساخت سازمانی شامل هزینه‌های مورد نیاز افراد جهت حفظ امنیت اطلاعات
پ) واپایش‌های امنیت اطلاعات (مانند هزینه راه‌حل‌های مدیریت دسترسی کاربر، هزینه رمزنگاری پشتیبان‌ها) حمایت مداوم کافی را مطابق با گرایش سازمان به مخاطره (مانند مخاطره باقیمانده پذیرفته‌شده) تامین می‌کند.
ت) فعالیت‌هایی جهت فراهم کردن آزمون واپایش مداوم، تضمین فرایند و یا صدور گواهی برای نشان دادن آنکه امنیت اطلاعات به یک استاندارد خاص دست‌یافته است.
ث) توسعه فرهنگی، آموزش و آگاه‌سازی که منجر به کاهش تعداد رخدادهای مربوط به امنیت اطلاعات می‌شود.
یادآوری- توجه سرمایه‌گذاری در زیرساخت‌های سازمانی و آموزش اثر آهسته اما بلندمدت بر سازمان دارد. بنابراین توصیه می‌شود در طول یک دوره زمانی طولانی‌تر به ارزیابی آن‌ها پرداخته شود.

۷ اهداف اقتصادی

۷-۱ مقدمه

کاربرد علم اقتصاد برای مدیریت امنیت اطلاعات نیازمند داده‌های مناسب از جانب برنامه مدیریت امنیت اطلاعات به‌کار رفته به‌عنوان عوامل ورودی در ابزارهای تصمیم‌گیری مورد استفاده سازمان است. این فرایند برای ملاحظات اقتصادی مالی ساده است، اما برای ملاحظات غیرمالی دشوارتر است.

تصمیمات اقتصادی اولویت‌بندی کالاهای محدود در دسترس و منابع خدمات را جهت بهینه‌سازی دستیابی به اهداف سازمانی شامل می‌شود. این تصمیمات اقتصادی برای مدیریت امنیت اطلاعات و سایر بخش‌های سازمان به‌طور مساوی به‌کار می‌روند.

پیوست ب نمونه‌هایی از عوامل تصمیم خاص امنیت اطلاعات را برای بررسی در هنگام بهینه‌سازی دستیابی به اهداف چندگانه به‌کار می‌برد. هر تصمیم‌گیری مربوط به هزینه از پتانسیل اثرگذاری بر دستاوردهای نتایج امنیت اطلاعات برخوردار است. به‌عنوان مثال سرمایه‌گذاری فزاینده در کاهش مخاطره به سازمان این امکان را می‌دهد تا با مخاطره پایین عمل کنند، احتمال بهبود حساسیت متقابل سازمان نسبت به تغییر وجود ندارد.

۷-۲ ارزش‌گذاری نسبت به تغییر دارایی‌های اطلاعاتی

توصیه می‌شود ارزش‌گذاری دارایی‌های اطلاعاتی با هدف امنیت اطلاعات، در مقایسه با معیارهای محرمانگی، یکپارچگی و دسترس‌پذیری (و همه جنبه‌های اضافی امنیت اطلاعات مورد نیاز سازمان) انجام شود. هنگام تعیین ارزش در اقلام پولی، توصیه می‌شود اگر مصالحه‌ای در معیار واقعی شد، در این صورت این ارزش، ارزش تاثیر کسب‌وکار دارایی را منعکس سازد. به‌عنوان مثال اگر یک وبگاه عمومی دارای یکپارچگی نباشد (یعنی اطلاعات آن وبگاه گمراه کننده باشند)، ممکن است یک اثر خاص داشته باشد که می‌توان آن را به صورت اقلام پولی بیان کرد. ارزش محرمانه بودن در اقلام پولی در همان وبگاه صفر است در حالتی که اطلاعات به‌طور عمومی در دسترس هستند. اگر همان وبگاه در دسترس نباشد، اثر تجاری به دلیل عدم دسترس بخش‌های خارجی به اطلاعات اثر متفاوتی بر اقلام پولی خواهد داشت. بنابراین سه ارزش متفاوت برای این دارایی وجود دارد. توصیه می‌شود این راهنما را در هنگام اجرای ارزشیابی دارایی در نظر گرفت.

از آنجایی‌که ارزشیابی دارایی‌های ناملموس دشوار است دو رویکرد ساده وجود دارد که می‌توان از طریق استفاده از یک مقیاس تطبیقی مانند پایین، متوسط، بالا، یا یک مقیاس عددی مانند ۱-۴ اتخاذ کرد. این نوع ارزشیابی به‌طور خاص زمانی مناسب است که ارزش‌ها و / یا هزینه‌ها محاسبه شوند و / یا به صورت گستره ارزش‌ها (بیشینه یا کمینه) ارائه شوند.

ممکن است مقادیر اقتصادی به صورت توجیه‌پذیری اقتصادی مرتبط با دارایی‌هایی ملموس و ناملموس برای سرمایه‌گذاری امنیت اطلاعات به‌کار روند که در جدول ۲ رده‌بندی شده است.

جدول ۲- انواع ارزش‌های اقتصادی سازمانی

نوع ارزش	توصیف
فیزیکی	مجموع دارایی‌های ملموس که متشکل از یک سازمان است
مشتری	ارزش کسب‌وکار توسط گروهی از مشتریان مشخص می‌شود
اجتماعی	ارزشیابی درکی که جامعه به‌طورکلی از آن سازمان دارد (ارزشی که به صورت کلان، جامعه از سازمان دارد)
شهرت	ارزشیابی درکی که رقبا، تامین کنندگان، مشتریان، ذی‌نفعان، دولت‌ها و سایر مولفه‌های ذی‌نفعان از سازمان دارند
ناملموس/منطقی	مجموع دارایی‌های ناملموس که یک سازمان را تشکیل می‌دهد. توصیه می‌شود دارایی‌های ناملموس، اطلاعات سامان‌دهی شده توسط سازمان را شامل شود: راهبردی، کسب‌وکار و غیره
قانونی و مقرراتی	تحریم‌های بالقوه و یا جرایم ناشی از نقص

توصیه می‌شود مدل اصلی ارزش را به همراه ترازنامه برای ارزشیابی و ارائه نتیجه‌گیری‌های اقتصاد امنیت اطلاعات به‌کار برد و این بر مبنای ویژگی‌های زیر است:

ارزش‌های مستقیم ارزش‌های اقتصادی مستقیم مانند زیان در مواد، یا سرمایه‌گذاری مستقیم مبتنی بر یک وقوع هستند که می‌تواند مجهول یا معلوم باشد. ارزش‌ها در این قسمت باید دقیق باشند.

ارزش‌های غیرمستقیم توسعه‌ای از ارزش‌های مستقیم هستند و ارزش‌های ناملموس‌تر و اضافی ازدست‌رفته یا به‌دست‌آمده را نشان می‌دهد.

ارزش‌های غیرمستقیم عدم قطعیت بیشتری داشته و به‌این‌ترتیب می‌تواند درون محدوده قرار گیرد. این ارزش‌ها ممکن است شامل ارزش خروجی ازدست‌رفته، سرپرستی افزایش‌یافته و غیره شود.

ارزش‌های توسعه یافته، آن ارزش‌هایی هستند که از ارزش‌های مستقیم و غیرمستقیم تاثیر پذیرفته و می‌توانند کاملا بااهمیت باشند. ارزش‌های توسعه یافته، دارای گستره بیشتری بوده و باید مبتنی بر همان مبنای ارزش‌های مستقیم و غیرمستقیم ارزشیابی شوند، ولی از عوامل دیگری همانند عوامل موثر بر جامعه و یا کل سازمان تاثیر می‌پذیرند. اغلب اوقات ارزش‌های توسعه یافته به‌عنوان ارزش‌های مقبول همانند نشان تجاری، شهرت و غیره در نظر گرفته می‌شوند (توجه داشته باشید که به احتمال زیاد ارزش‌های توسعه یافته منفی هستند اما گاهی ممکن است مثبت نیز باشند.)

توصیه می‌شود یک سازمان ارزشیابی خود را از دارایی اطلاعاتی از طریق بررسی ذی‌نفعان مختلف تکمیل کند که این ذی‌نفعان دربرگیرنده موارد زیر هستند:

الف) دارایی‌های ملموس که یک سازمان را تشکیل می‌دهند.

ب) ارزش ایجاد شده توسط مجموعه اوراق بهادار مشتریان

پ) دارایی‌های ناملموس مثل اطلاعات، درک و دریافت مشتری، ارزش برچسب تجاری، استنباط اجتماعی

جدول۳-انواع ارزش‌های دارایی‌های اقتصادی-اصول و مثال‌ها

رده	نوع ارزش	توصیف	دارایی	ارزش
الف	سازمان	طرف‌های درون محدوده ISMS	دارایی‌ها تعریف می‌شوند تا بتوان یک کار را در طول زمان اجرا و حفظ نمود.	ارزش کل را می‌توان برای فرآیندهای کاری مرتبط با دارایی‌های خاص مانند حقوق مالکیت معنوی، دادگان، منابع ICT و غیره بخش‌بندی کرد و ارزش‌ها را برای آن‌ها به‌کار برد.
ب	طرف‌های دوم و سوم	تک‌تک مشتری‌ها و تامین کنندگان	دارایی‌ها که باید تعریف شوند تا بتوان کار را در ارتباط با یک گروه مشخص اجرا و حفظ نمود	ارزش تعریف‌شده برای دارایی‌ها را شامل می‌شود
پ	ذی‌نفعان	هر گروه علاقه‌مند جنبه‌های امنیت اطلاعات سازمان، همانند مالکان دارایی‌ها باید تعریف شوند تا بتوان کسب‌وکار را در ارتباط با یک گروه مشخص اجرا و حفظ نمود	دارایی‌هایی که برای اجرا و نگهداری در ارتباط با طرف معین تعریف‌شده‌اند	ارزش کل را می‌توان برای فرایندهای کسب‌وکار مرتبط با دارایی‌ها خاص مانند IPR، دادگان، منابع ICT، و غیره بخش‌بندی کرد و ارزش‌ها را برای آن‌ها به‌کار برد
ت	اجتماعی	سودهای تعیین‌شده جامعه	دارایی‌ها می‌توانند سود تعیین‌شده یک جامعه را تشکیل دهند.	ارزش تاثیر بر جامعه چیزی است که می‌توان آن را بعدا به سازمان منتقل کرد.

همچنین این ارزشیابی را می‌توان به‌منظور کاربرد ترکیب مناسبی از طبقات مربوط رتبه‌بندی کرد. به‌عنوان مثال دارایی‌های اطلاعاتی مربوط با دادگان ۱۰۰۰۰۰ سند مشتری محتوی اطلاعات قابل شناسایی به‌طور شخصی در هنگام تجمیع سودهای تعیین شده سازمانی (رده الف) ، ذی‌نفعان (رده پ)، و سایر گروه‌ها تحت تاثیر (رده ب)، بسیار ارزشمندتر می‌شود.

ممکن است ارزشیابی بر اساس طبقات دارایی‌های مهم درجه‌بندی شود. به‌عنوان مثال دادگان ۱۰۰۰۰۰ سند مشتریان حاوی اطلاعات قابل شناسایی برای یک بخش دولتی بسیار مهم هستند. به‌طور مشابه، گزارش‌های نهایی منتشرنشده‌ی یک شرکت بین‌المللی بسیار حساس خواهد بود، و خطر معامله بر اساس اطلاعات محرمانه و تبعات مهم اقتصادی بین‌المللی در آن وجود دارد.

سازمان‌ها می‌توانند با طراحی رابطه بین تصمیمات هزینه و پیامدهای مربوطه تصمیمات اقتصادی آگاهانه اتخاذ نمایند. در این صورت هزینه تصمیم (مانند هزینه‌های کاهش مخاطره، هزینه‌های صدور گواهی‌نامه) پیامدهای متعددی دارند و نشان دادن این رابطه در یک جدول امکان‌پذیر است.

۸ تراز نمودن اقتصاد امنیت اطلاعات برای ISM

۸-۱ مقدمه

یک سازمان دارای عملکرد مطلوب، به سامانه مدیریت امنیت اطلاعاتی نیاز دارد که باقی ماندن دارایی‌های اطلاعاتی حفاظت شده از حوادث نامطلوب را تضمین کند و همزمان برای کسانی که به کاربرد اطلاعات برای تحویل سازمانی قابل دوام اهداف کسب‌وکار نیاز دارند در دسترس می‌باشد. الزامات متداول مرتبط با تعیین منافع و هزینه‌هایی که سازمان برای رسیدن به اهداف کسب‌وکار باید به آن دست پیدا کند، با موارد زیر مرتبط است:

الف) کاهش زیان (اغلب اوقات سالیانه)

ب)کمینه کردن هزینه‌های مربوط به اقدامات احتیاطی مالی و غیره برای وقوع ضرر (حوادث)

پ)اثربخشی برنامه مدیریت امنیت اطلاعات طراحی شده برای حفاظت دارایی‌های اطلاعاتی

ت)کارآمدی برنامه امنیت اطلاعات در ارتباط با هزینه برنامه‌ریزی، طراحی، پیاده‌سازی، نگهداری و ارتقای برنامه.

برنامه مدیریت امنیت اطلاعات می‌تواند منافع ناملموس/غیرمالی و ملموس/مالی با مقادیر مثبت را ایجاد نمایند در این صورت مدیریت توانایی برای هدایت و واپایش مخاطرات امنیت اطلاعات را حفظ می‌کند.

توصیه می‌شود تصمیم‌گیری‌های مربوط به هزینه و منفعت، با منافع مورد انتظار از دست یافتن به کاهش مخاطره از طریق استقرار واپایش‌های برنامه‌ریزی‌شده مرتبط باشد. عموما، مخاطرات با استفاده از تعدادی واپایش کاهش می‌یابند. ممکن است استقرار یک واپایش خاص، در سطوح مختلف کاهش مخاطره مشارکت داشته باشد، و از مشارکت جزئی تا کاهش کامل مخاطره تغییر کند.

توصیه می‌شود امنیت اطلاعات، دستیابی به اهداف کسب‌وکار را مورد حمایت قرار دهد. توصیه می‌شود به خاطر داشت که رویکردهای متفاوت را می‌توان با هزینه‌ها و منافع متفاوت اتخاذ کرد تا دستیابی به اهداف تجاری مطلوب را امکان‌پذیر سازد. به‌عنوان مثال احتمال دارد سرعت فدا کردن منافع بازار (مثل افزایش سریع درآمد) با افزایش هزینه‌های بالقوه زیان امنیت اطلاعات امکان‌پذیر شود (مثلا خصوصی بودن دادگان مشتری جدید مورد حفاظت قرار نمی‌گیرد و توسط افراد غیرمسئول قابل دسترسی است). در این مورد زیان بالقوه، ارزشیابی از زیانی را ارائه می‌دهد که احتمال دارد در غیاب یا سازش دارایی‌های اطلاعاتی (دادگان) موجب شود. به‌عنوان راهی دیگر ممکن است پذیرش هزینه بالاتر برنامه مدیریت امنیت اطلاعات برای شناسایی منافعی مورد پذیرش باشد که با پذیرش خوب یک محصول یا خدمات همراه است.

۸-۲ منافع اقتصادی

کاهش در زیان‌ها می‌تواند به‌وسیله مقایسه ضرر سالیانه پیش‌بینی‌شده در غیاب و حضور برنامه مدیریت امنیت اطلاعات تحت بررسی، تعیین شود. لازم است در هنگام اجرای این مقایسه بررسی‌هایی با استفاده از یک روش شناختی ارائه گردد که می‌تواند با دیگر روش شناختی‌های مورد استفاده سازمان همسو باشد.

هر جا فنون ارزیابی یا معیارهای متفاوت برای شناسایی مخاطره امنیت اطلاعات به‌کار روند، احتمالا کل نتایج اقتصادی سازگار و یکپارچه نبوده و با سایر برنامه‌ها و ابتکارات قابل مقایسه نیستند. همچنین برای

تضمین یک نتیجه سازگار و قابل قیاس معیار مخاطره به‌کار رفته برای تعیین منافع اقتصادی توصیه می‌شود بر مواردی محدود شود که تمرکز مالی دارند بنابراین توصیه می‌شود سازمان نحوه کاربرد عوامل اقتصادی غیرمالی را هنگام تکمیل تمرکز اقتصادی مالی مدنظر قرار دهد. اطلاعات مربوط به مدیریت مخاطرات امنیت اطلاعات را می‌توان در استاندارد ملی ایران به شماره ۲۷۰۰۵: سال ۱۳۹۲ یافت.

شایان توجه است که انتخاب معیار مخاطره‌ی مرتبط با تعیین منافع اقتصادی مالی، به‌ندرت در عملکرد مدیریت امنیت اطلاعات جای می‌گیرد و اغلب اوقات به‌وسیله مدیر ارشد مالی یا شخصی با وظیفه مالی مشابه مشخص می‌شود.

ممکن است هزینه‌های مربوط به کمینه‌سازی ضرر مالی و سایر تدارکات برای وقوع زیان، به‌عنوان پیامد برنامه مدیریت امنیت اطلاعات، کاهش یابند. این یک منفعت اقتصادی است که می‌توان آن را هنگام ارزیابی برنامه پیشنهادی مدیریت اطلاعات به حساب آورد.

۸-۳ هزینه‌های اقتصادی

هزینه‌های برنامه مدیریت امنیت اطلاعات برای حفاظت اهداف تجاری خاص باید کل چرخه حیات برنامه را با استفاده از یک رویکرد مبتنی بر مخاطره پوشش دهد. فضاهایی که توصیه می‌شود تحت پوشش قرار گیرند شامل موارد زیر می‌شوند:

الف) برنامه‌ریزی

ب) پیاده‌سازی

پ) عملکرد

ت) حفظ

ث) اصلاح

ج) از اختیار ساقط کردن

توصیه می‌شود روال‌های گزارش‌گیری و تضمین (شامل هر گونه ممیزی توسط مشتریان، ممیزی داخلی طرف‌های سوم یا سایر روال‌های تضمین) نیز در هزینه‌ها گنجانده شوند. همچنین توصیه می‌شود هزینه‌های مربوط به آموزش و حفظ آگاهی‌رسانی در زمینه عملکرد مردم یا استفاده از واپایش‌های امنیت اطلاعات در هزینه‌ها گنجانده شود.

همچنین هزینه‌ها باید کل برنامه مدیریت امنیت اطلاعات را پوشش داده و نه فقط با منافع اقتصادی بلکه با سنجش تثبیت شده پیش از حصول آن مرتبط باشد (به استاندارد ISO / IEC 27004 مراجعه شود). اغلب اوقات اتخاذ این رویکرد برای جداسازی هزینه‌ها در طبقات مرتبط با منافع اقتصادی و سایر منافع واقع‌گرایانه نیست.

حفظ اطلاعات و آگاهی درباره هزینه‌ها و اثربخشی برنامه مدیریت امنیت اطلاعات منفعت اضافی تامین می‌کند که سازمان را قادر می‌سازد تا اطمینان را بیان نموده و به ذی‌نفعان سازمانی اعتماد نمایند.

توصیه می‌شود فضاهای اصلی هزینه را هنگام ارزیابی برنامه مدیریت امنیت اطلاعات مورد بررسی قرار داد (جدول ۴).

جدول ۴- فضاهای اصلی هزینه

فضای هزینه	توصیف
ارزیابی مخاطره	همه هزینه‌های مربوط به شناسایی، تحلیل و ارزیابی مخاطره را دربر می‌گیرد.
آموزش و آگاهی	آموزش برای آشنایی، برنامه سرتاسر کمپانی، آموزش هدف‌دار، ارزیابی آموزش، بازنگری‌ها ، توسعه ماده آموزشی، ارائه‌دهندگان و ابزارهای پایش را شامل می‌شود.
واپایش‌ها	هزینه‌های مستقیم برای انتخاب و پیاده‌سازی واپایش‌ها را جهت کاهش مخاطرات، عمل کردن واپایش‌ها، سایر گزینه‌های برطرف‌سازی مخاطره، و هزینه‌های غیرمستقیم مرتبط با اثر کارآمدی مربوط به واپایش را در بر می‌گیرد ممکن است واپایش‌ها بازدارنده، کشف کردنی و یا واکنشی باشند.
گواهی	هزینه‌های مربوط به پایش و آزمون، کارکردهای بیمه، آزمودن گواهی و هر چیزی را که برای معتبر ساختن اثربخشی واپایش‌ها امنیت کار می‌کنند را در بر می‌گیرد. هزینه‌های گواهی بر مبنای هزینه کارکنان (اجرای آزمون واپایش) هزینه حسابرسی‌ها، هزینه گواهی‌های نگهداری یا ثبت‌نام‌ها توسط نهادهای مجاز
ممیزی	هزینه‌های منابع ممیزی (خارجی و / یا داخلی) را دربر می‌گیرد و توصیه می‌شود هزینه زمانی کارکنان را برای حسابرسی و نیز برنامه‌ریزی، حمایت و پیگیری را شامل شود.
سنجش	هزینه‌های منبع یابی داخلی و خارجی برای برنامه‌هایی سنجش، ابزارها و کاربردهای آن‌ها را شامل شده و باید هزینه زمان کارکنان داخلی را برای آماده کردن نتایج سنجش در بر گیرد.

۸-۴ کاربرد محاسبات اقتصادی برای ISM

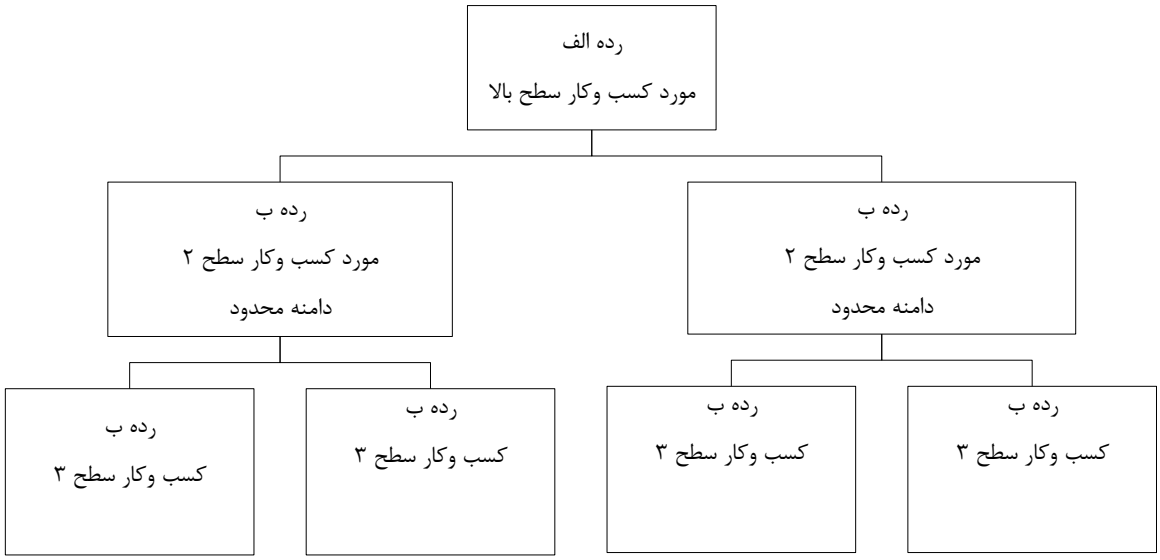
۸-۴-۱ مرور کلی

یک مورد کسب‌وکار را باید برای دستیابی به اهداف امنیت اطلاعات ارائه کرد که اقتصاد امنیت اطلاعات مبتنی بر مدل محاسبه را شامل می‌شود. به پیوست پ مراجعه شود.

توصیه می‌شود منطق کسب‌وکار اقتصادی برای سرمایه‌گذاری‌های امنیت اطلاعات، شامل هزینه‌ها، درآمدها، بازده باشد. مثلا دلیل منطقی کسب‌وکار برای پذیرش هزینه‌ها و سرمایه‌گذاری‌ها در آن گنجانده شود.

همچنان‌که یک مدل منحصربه‌فرد است، رویکرد خاص یک مورد را نیز توصیه می‌شود در نظر گرفت. اقتصاد امنیت اطلاعات با اقتصاد به‌کار رفته برای توجیه سرمایه‌گذاری طراحی شده جهت استفاده از بازار به‌منظور خلق اثر فروش‌ها چندان متمایز نیست. منفعت در قالب درآمد و بازده به‌ندرت دیده می‌شود و باید برآورد گردد.

همان‌طور که در بند ۶-۲ توصیف شده موارد تجاری را می‌توان به دو نوع رده‌بندی کرد. کاربرد مدل‌ها برای یک مورد را می‌توان به صورت سلسله مراتبی در شکل ۲ مشاهده کرد. این روش در چند لایه به‌کار می‌رود و اگر مناسب باشد، تجمیع می‌شود. استفاده از تجمیع در مورد کسب‌وکار رده ب آسان‌تر است زیرا دامنه کاربرد محدودتری دارد.



شکل ۲– رویکرد «پایین به بالا» برای تفسیر یک مورد کسب‌وکار مدیریت امنیت اطلاعات

بزرگ‌ترین تفاوت در هنگام کاربرد یک مدل اقتصادی آن است که گستره سازمانی رده (الف) اغلب به صورت «بالا به پایین» به‌کار می‌رود، درحالی‌که رده (ب) دامنه بسیار اندکی داشته و رویکرد «پایین به بالا» به کار برده می‌شود.

اگر داده‌های دقیقی در دسترس باشد، مدل برای گستره سازمانی رده (الف) را می‌توان با مدل‌های مفصل‌تر حمایت کرد. دقت و صحت محاسبات در هنگام کاربرد گستره سازمانی رده (الف) یا مدل بخشی (ب) از عوامل زیر تاثیر می‌پذیرد:

الف)دسترس‌پذیری اطلاعات موجود مرتبط با محاسبه اقتصاد همانند ارزش دارایی‌ها، آمار، و غیره

ب)منابع در دسترس برای نتایج مانند زمان، افراد، امور مالی

پ)دسترسی‌پذیری اطلاعات تجاری مانند تخصص، خارجی، داخلی

یک رویکرد ساده را می‌توان به صورت نقطه آغاز برای رده‌بندی به‌کار برد و سپس محاسبه اقتصاد را بر مبنای محاسبه اولیه بسط داد.

۸-۴-۲ راهنما

توصیه می‌شود مراحل زیر را به‌عنوان بخشی از ISM به‌منظور شناسایی دلیل منطقی تجاری و استفاده روش‌های اقتصادی تحت عنوان «مورد» به‌کار برد:

الف) تعیین کردن محتوا

۱) اتخاذ کسب‌وکار مبتنی بر توصیف درصورتی‌که در دسترس باشد.

۲) تعیین دامنه کاربرد مورد

۳) تعیین محتوای مورد

۴) تعیین کردن ذی‌نفعان

۵) تعیین کسانی که توصیه می‌شود در مورد کسب‌وکار تصمیم‌گیری کنند

۶) مشخص کردن رده مورد

ب) شناسایی دارایی‌هایی که در دامنه کاربرد مورد از امنیت اطلاعات تاثیر می‌پذیرند:

۱) اطلاعات مهم

۲) سامانه ICT

۳) مشخص کردن هر نوع سرمایه دیگر

۴) ارزش امنیت اطلاعات دارایی‌هایی که توصیه می‌شود برای دارایی‌های مشخص شده به صورت فهرست بیان شود.

۵) رویکرد مبنای به‌کار رفته برای محاسبه دربرگیرنده مدل‌ها و تجمیع

پ) مشخص کردن اهداف مورد

۱) توصیف در قالب اصطلاحات مربوط به کیفیت

۲) توصیف در قالب اصطلاحات مربوط به کمیت

۳) نتیجه‌گیری در قالب اصطلاحات پولی

ت) مشخص کردن زمان

۱) مدت زمانی که انتظار می‌رود مورد بر سازمان اثر داشته باشد

الف) موارد بلندمدت – بیشتر از یک سال، اگر چنین باشد، چند سال.

ب) کوتاه‌مدت – بیشینه یک سال

ث) مشخص کردن هزینه‌هایی برای کاربرد مواردی مانند :

۱) هزینه‌های کوتاه‌مدت (بیشتر از یک سال به‌کار نرود و پس از آن هیچ تاثیری بر سازمان نخواهد داشت)

۲) هزینه‌های سرمایه‌گذاری (هزینه‌های یک‌باره که در حین اجرای مورد بر آن تاثیر خواهد داشت).

۳) هزینه‌های جاری – هزینه‌های سالیانه برای مورد در طول دوره زمانی آن

۴) پرداختن به هزینه‌هایی مانند هزینه‌های مستقیم، هزینه‌های غیرمستقیم یا هزینه‌های گسترده مفید است (به مدل پ-۳ مراجعه کنید).

ج) مشخص کردن منافع و ارزش مورد مانند:

۱) منافع انطباق به‌وسیله اجتناب از جرایم

۲) فرصت‌های انطباق/ فروش‌ها از طریق جذب بازارهای جدید

۳) فرصت‌های تصویر/ فروش از طریق جذب بازارهای جدید

۴) ارزش مثبت کاهش مخاطره

۵) ارزش افزایش کارایی داخلی

۶) ارزش امنیت اطلاعات هر دارایی درصورت توافق

۷) هر مورد قابل مقایسه دیگر

۸) برای ارزش، مفهوم منفی شدن هزینه را می‌توان به صورت ارزش فرصت به‌کار برد (به

پیوست پ مراجعه کنید).

چ) از امکان برهم‌کنش بین هزینه و ارزش استفاده نمایید.

ممکن است همه موارد فوق کاربست‌پذیر باشد ولی اغلب اوقات به دلیل زمینه‌ی مورد، فقط به کار بردن بعضی از ارزش‌ها معنا می‌پذیرد. اطلاعات درباره ارزش‌ها از منابع مختلف اما مرتبط ناشی می‌شوند. به‌عنوان مثال، ممکن است ارزش کاهش مخاطره، جرایم انطباق را دربرگیرد. اغلب اوقات ارزش امنیت اطلاعات نیز بازتاب پیامدهای مرتبط با مخاطره باشد. احتمال دارد در عمل منابع بسیاری مورد استفاده قرار گیرند.

مبنا را برای روش منتخب قطعی نمایید.

۱) اگر محتوا و دامنه کاربرد کل سازمان باشند، روشی مانند BVM و یا/محاسبه سرمایه‌گذاری عمومی مناسب است. ترکیبی از این دو چندان نامعمول نیست (مرجع رده الف مورد کسب‌وکار).

۲) اگر محتوا و دامنه کاربرد محدود و دارایی/ واپایش متمرکز باشد، روشی مانند RIO را می‌توان به‌کار برد (مرجع رده ب مورد کسب‌وکار).

۳) اگر محتوا و دامنه کاربرد ترکیبی از موارد فوق باشد، هر دو روش فوق را می‌توان به‌کار برد، اما نیاز به بررسی دارایی‌ها و اثرات CIA آن‌ها وجود دارد (مرجع رده ب مورد کسب‌وکار).

۸-۴-۳ مورد کسب‌وکار مبتنی بر رویکرد کل سازمان (رده الف)

یک مورد گسترده‌تر (رده الف را می‌توان از طریق مقادیر اقتصادی تجزیه شده به جزئیات و سپس تجمیع (پایین به بالا) یا استفاده مشخص از تحلیل روش بازنگری (روش بالا به پایین) به‌کار برد. احتمالا روش آخری عدم قطعیت بسیاری را شامل می‌شود که ممکن است آن را بی‌اعتبار کند. درحالی‌که تاثیر دقیق بودن برای تصمیم‌گیری مدیریت به دست می‌دهد. اما این عمل بدون ارائه نتایج کمی مقصود و بسیار زمان‌بر خواهد بود.

این روش را می‌توان در چند مرحله پیاده‌سازی نمایید. به‌طورکلی این روش، فرایندی قابل تکرار همراه با ورودی‌های متغیر در حین جمع‌آوری اطلاعات است، بنابراین تغییرات قبل از انجام محاسبات نهایی رخ می‌دهد. اغلب اوقات شناسایی گستره‌ای از ارزش‌های ورودی‌ها یا نتایج آسان‌تر از ارزش‌های دقیق است. هر جا یک گستره به‌کار رود، ثبت مقادیر احتمالی بیشینه یا کمینه مفید خواهد بود.

ورودی مثبت

الف) ارزش مستقیم فرصت سالیانه مانند پیشامد کاهش هزینه

ب) ارزش غیرمستقیم فرصت به‌کار رفته در دوره زمانی مورد، مانند اجتناب از جرایم به‌وسیله انطباق

پ) ارزش گسترده فرصت به‌کار رفته در دوره زمانی مورد، مانند فرصت‌های فروش برای بازار جدید

ورودی منفی

ت)۱. هزینه‌های مستقیم سالیانه، مانند هزینه‌های جاری

ث)۲. هزینه‌های غیرمستقیم به‌کار رفته در طول دوره زمانی مورد، مانند برپاسازی پروژه

ج)۳. هزینه‌های گسترده به‌کار رفته در طول دوره زمانی مورد، مانند زبان فروش

برای مثال به ت-۱ رجوع کنید (مدل اشاره شده در پ-۲ و پ-۵ به‌کار می‌رود)

همچنین این را می‌توان بر اساس دارایی‌های دامنه کاربرد (روش پایین به بالا) با استفاده از اصل جدول دو محاسبه کرد. این رویکرد بسیار دقیق‌تر خواهد بود اما کار گسترده‌تر می‌شود و به دارایی‌های مشخص شده بستگی دارد، در بسیاری از نمونه‌ها به سهولت در دسترس نیست. بر اساس شکل ۲ این رویکرد، رویکرد "پایین به بالا" نام دارد.

۸-۴-۴ مورد کسب‌وکار مبتنی بر یک بخش سازمان (رده ب)

یک مورد محتوایی جزیی (رده ب) به این معنی است که همه ارزش‌های اقتصادی باید در یک سطح مفصل جمع‌آوری گردد، و سپس تجمیع شوند (پایین به بالا).

ممکن است پیچیدگی مورد رده جزیی (رده ب) بیش از حد تغییر کند. مدل‌های ت-۲ و ت-۳ کاربرد دامنه کوچک و بعد دامنه گسترده‌تر را نشان می‌دهند.

این روش را می‌توان به صورت چند مرحله‌ای به‌کار برد. به‌طورکلی این روش یک فرایند قابل تکرار همراه با ورودی‌های متغیر در حین جمع‌آوری اطلاعات است. محاسبه نهایی را نمی‌توان تا زمان تکمیل تغییرات انجام داد. اغلب اوقات شناسایی گستره‌ی ارزش‌های ورودی یا نتایج نسبت به ارزش‌های دقیق آسان‌تر است. هر جا یک گستره به‌کار رود، ثبت مقادیر احتمالی بیشینه یا کمینه مفید خواهد بود.

ورودی مثبت

الف) ارزش CIA دارایی / دارایی‌ها در دامنه کاربرد مورد کسب‌وکار

ب) تشخیص و شناسایی اثر بر ارزش یا به حساب آوردن مخاطره CIA

پ) تبدیل یک تاثیر منفی بر یک ارزش فرصت با فرض سطوح صحیح امنیت اطلاعات برای هر کدام از فرانامه‌های دسترس‌پذیری و درستی، اطمینان‌بخش بودن (مثلا هیچ‌کدام از مخاطرات شناسایی‌شده تحقق نیابد)

ورودی منفی

ت) هزینه‌های مستقیم سالیانه مانند هزینه‌های فعلی برای کاهش مخاطرات

ث) هر هزینه غیرمستقیم به‌کار رفته در طول دوره مورد کسب‌وکار همانند برپاسازی یک پروژه

ج) هزینه‌های گسترده به‌کار رفته در طول دوره زمانی مورد کسب‌وکار مانند ضرر فروش

به مثال ت-۲ رجوع کنید.

مورد کسب‌وکار محتوای جزئی (رده ب) با دامنه کاربرد محدود، به آن معناست که همه مقادیر اقتصادی را باید در یک سطح مفصل جمع‌آوری نمود، تا بعدا به‌طور مستقیم برای این مورد به‌کار رود.

یک تحلیل کوتاه طرح‌ریزی نموده و روش ساده‌ای همانند مدل منفی به مثبت را انتخاب کنید که به سرعت اجرا و شناسایی می‌شود(به پ-۵ مراجعه نمایید.)

ورودی مثبت

الف) تاثیر واقعی یا بالقوه تجارت را در ارتباط با امنیت اطلاعات برآورد کنید.

ب) ارزش مثبت را برای فعالیت مورد کسب‌وکار برآورد کنید.

پ) در صورتی نتیجه‌گیری نمایید که بسته به فعالیت احتمال وقوع ارزش‌های مثبت دیگر وجود داشته باشد

و تصمیم بگیرید آن‌ها را بگنجاند یا خیر. این به مورد کسب‌وکار و اطلاعات در دسترس بستگی خواهند داشت.

ورودی منفی

ت) واپایش‌های مستقیم و غیرمستقیم مورد نیاز برای کاهش اثر را شناسایی کنید.

ث) هزینه‌های مستقیم و غیرمستقیم را جهت به‌کار بردن واپایش‌ها معین کنید.

نتیجه‌گیری

ج) تعیین ارزش/ هزینه‌های خالص

چ) مقایسه و تصمیم‌گیری

به ت-۳ مراجعه کنید.

پیوست الف
(اطلاعاتی)
شناسایی ذی‌نفعان و هدف‌ها برای تنظیم ارزش‌ها

الف-۱ مرور کلی

هدف این پیوست کمک به سازمان‌ها در جهت فهم و شناسایی اثر گسترده‌تر اقتصادی برنامه‌های مدیریت امنیت اطلاعات آن‌ها و سرمایه‌گذاری‌های مربوطه است. مجموعه‌ای از حوزه‌های مختلف وجود دارد که می‌توانند از بهبود مدیریت امنیت اطلاعات سازمان بهره ببرند.

ماهیت و اندازه منفعت اقتصادی، بستگی به نحوه استفاده سازمان از منافعی دارد که می‌تواند در ارتباط با مدیریت مناسب‌تر امنیت اطلاعات به‌دست آورد.

الف-۲ بخش‌های خصوصی یا عمومی مهم

سازمان‌های بخش عمومی و خصوصی در بخش‌های صنعتی که در آن‌ها امنیت اطلاعات هدف اصلی کسب‌وکار است (مانند بانکداری، دولت، بهداشت و دفاع) به برقراری و حفظ امنیت اطلاعات به‌عنوان بخش اصلی ارزش و وجه علامت تجاری آن‌ها بستگی دارد و در حقیقت بخش ذاتی محصولات و خدمات آن‌ها می‌باشد. اگر سازمان‌ها در چنین بخش‌هایی از حوادث امنیت اطلاعات دچار آسیب شوند و علامت تجاری آن‌ها دستخوش ضرر شده احتمال دارد در بدترین موارد از صحنه کار خارج شوند.

الف-۳ امنیت و بهداشت عمومی

استاندارد پیشنهادی به روشنی بر بهداشت و امنیت اثری ندارد. از این رو به‌طور غیرمستقیم بر امنیت بسیاری از اشکال درمان پزشکی از طریق تضمین اطلاعات اثر می‌گذارد که اطلاعات در چنین درمانی مبتنی بر دریافت[1] کافی حفاظت امنیت است.

الف-۴ اجتماعی و جامعه

استاندارد پیشنهادی به طرز گسترده‌ای برای سازمان‌هایی به‌کار می‌رود که با همه بخش‌های اجتماع سروکار دارند. احتمال داشتن یک اثر مخالف بر گروه‌های اقلیت یا آسیب‌پذیر وجود ندارد و در حقیقت همه ذی‌نفعان اجتماع و به‌طورکلی جامعه سود خواهد برد.

الف-۵ اطلاعات شخصی

این استاندارد در مواردی که اطلاعات به افراد و امور شخصی آن‌ها می‌پردازد و اثر مفیدی خواهد داشت زیرا احتمال دارد حفاظت از افراد و اطلاعات حساس در سازمان‌هایی که از این استاندارد در ارتباط با سامانه مدیریت امنیت اطلاعات بهره می‌برند بهبود یابد.

مدیریت انبارهای گسترده اطلاعات شخصی یکی از فضاهایی است که اغلب سازمان‌ها در آنجا با چالش‌های بزرگ امنیت اطلاعات روبرو می‌شوند. یک حد بینابین امنیت اطلاعات فردی به نمودهای منفی منجر خواهد شد.

1- Receive

الف-۶ محیطی

استاندارد پیشنهادی به‌طور مستقیم به حد چشمگیری بر محیط موثر نخواهد بود.

استاندار پیشنهادی به‌طور غیرمستقیم بر محیط اثر مثبت می‌گذارد زیرا احتمال دارد اطلاعات حساس به مدیریت محیطی حمایت بهتری در سازمانی دریافت خواهند کرد که از استاندارد پیشنهادی در ارتباط با سامانه مدیریت امنیت اطلاعات بهره ببرد ممکن است در حال حاضر در عمل باشد.

الف-۷ رقابت

ممکن است سازمان‌هایی که از امنیت اطلاعات خوبی استفاده می‌کنند در مقایسه با سازمان‌هایی که از این سامانه استفاده نمی‌کنند به سود رقابتی دست یابند زیرا آن‌ها مخاطرات مربوطه را بهتر مدیریت می‌کنند.

پیوست ب

(اطلاعاتی)

تصمیمات اقتصادی و عوامل اصلی هزینه تصمیم‌گیری

مرجع	اهداف تجاری	تصمیمات هزینه‌ای			
		هزینه‌های کاهش مخاطره	هزینه‌های گواهی	هزینه‌های سازمانی مدیریت مخاطره	هزینه‌های واپایش
الف	ایجاد توانایی در کسب‌وکار جهت مشارکت در کارهای با مخاطره بالا، از طریق افزایش بلوغ در مدیریت مخاطره و عملکرد در مخاطره کمتر در مقایسه با رقبا	بله سامانه‌هایی با مخاطره پایین‌تر، مشارکت در محیطی با مخاطره بالا را امکان‌پذیر می‌سازند	بله ممکن است شرکای تجاری، مبتنی بر گواهی امنیت اثبات‌پذیر، برای مشارکت تحت تأثیر قرار گیرند	بله اگر سازمان بتواند سازمان مخاطره‌ی کامل‌تری را نشان دهد، احتمال زیادی وجود دارد که شرکای تجاری در فعالیت‌های اقتصادی با مخاطره بالاتر شرکت کنند	بله به‌طورکلی واپایش‌های به‌کار رفته مجموعه گسترده‌ای از واپایش‌هایی هستند که بر کل کار تجاری همانند آموزش اثر می‌گذارند هزینه برای هر واپایش به خود واپایش‌ها و کمال امنیت اطلاعات سازمان بستگی دارد.
ب	ایجاد توانایی در کار تجاری برای برآورده ساختن الزامات قانونی و در نتیجه اجتناب از محدودیت‌های منابع عملیاتی و جرایم از طریق بهبود و انطباق	بله سازمان‌هایی با کاهش دادن بهتر مخاطره موقعیت‌های قانونی بهتری دارند.	ممکن است گواهی به‌طور مستقیم جهت برآوردن الزامات قانونی مشارکت می‌کنند	خیر افزایش هزینه در مدیریت مخاطره سازمان مستقیماً به بهبود وضعیت قانونی منجر می‌شود	بله به‌طورکلی واپایش‌های به‌کار رفته مجموعه گسترده‌ای از واپایش‌ها می‌باشند که بر کل کار تجاری و نیز واپایش‌های فنی خاص اثر می‌گذارند هزینه برای هر واپایش به خود واپایش‌ها و کمال امنیت

مرجع	اهداف تجاری	تصمیمات هزینه‌ای			
		هزینه‌های کاهش مخاطره	هزینه‌های گواهی	هزینه‌های سازمانی مدیریت مخاطره	هزینه‌های واپایش
					اطلاعات سازمان بستگی دارد.
پ	ایجاد توانایی در کار تجاری برای چندمنظوره بودن ، چالاک بودن و حساس بودن نسبت به تغییر ، مثل ایجاد انعطاف‌پذیری در راه‌حل‌های امنیتی	خیر کاهش مخاطرات، سازمان را چالاک نمی‌سازد	خیر گواهی، چالاکی سازمان را بهبود نمی‌بخشد	بله افزایش مخارج در مخاطره عملیاتی سازمان کار تجاری را قادر می‌سازد تا فرصت‌های مخاطره بیشتری را به‌طور موثر مدیریت نمایند.	خیر به‌طورکلی واپایش‌ها در چالاکی سازمانی نقش ندارند. این بیشتر به ISM و کمال ISMS می‌پردازند.
ت	دستیابی به طرح قابل قبولی از ضررهای پیش بینی نشده در آینده بر مبنای نمایه مخاطره‌های مورد انتظار مثل کاهش مخاطره مبتنی بر ارزش مخاطره	بله کاهش مخاطره مستقیماً سطوح زبان مورد انتظار را به وجود می‌آورند	خیر – گواهی به‌طور مستقیم مخاطره پایین‌تر و نرخ زیان مورد انتظار را ایجاد نمی‌کند	بله افزایش مخارج در مقابله با مخاطره عملیاتی سازمان تا حد زیادی مخاطرات و زیان‌هایی را مورد انتظار را ایجاد نمی‌کند.	بله واپایش‌هایی را می‌توان به‌طور مستقیم برای کاهش مخاطره به‌کار برد
ث	انتظار زیان سالیانه (ALE)، محصول ارزش‌های مورد انتظار (ارزش‌های میانگین) از زیان‌ها و همچنین وقوع را بیان می‌کند. این‌گونه محاسبه سطح مخاطره نتایج موثری برای "رخدادهای با فراوانی پایین/ با تأثیر چشم‌گیر" فراهم نمی‌کند. اما، توصیه می‌شود واپایش‌های امنیت اطلاعات این	بله کاهش مخاطره مستقیماً سطوح زیان مورد انتظار را به وجود می‌آورد	خیر گواهی به‌طور مستقیم مخاطره پایین‌تر و نرخ زیان مورد انتظار را ایجاد نمی‌کند	بله افزایش مخارج در مقابله با مخاطره عملیاتی سازمان تا حد زیادی مخاطرات و زیان‌های مورد انتظار را کاهش می‌دهد	بله واپایش‌ها را می‌توان مستقیماً برای کاهش مخاطره به‌کار برد

مرجع	اهداف تجاری	تصمیمات هزینه‌ای			
		هزینه‌های کاهش مخاطره	هزینه‌های گواهی	هزینه‌های سازمانی مدیریت مخاطره	هزینه‌های واپایش
	"رخدادهای با فراوانی پایین/ با تأثیر چشم-گیر" را پوشش دهد. زیرا دغدغه حقیقی امنیت اطلاعات هستند. محاسبه ارزش در مخاطره (VAR) متوسط می‌تواند نتایج بهتری نسبت به ALE داشته باشد.				
ج	انتظار زیان سالیانه (ALE)، محصول ارزش‌های مورد انتظار (ارزش‌های میانگین) از زیان‌ها و همچنین وقوع را بیان می‌کند. این‌گونه محاسبه سطح مخاطره نتایج موثری برای "رخدادهای با فراوانی پایین/ با تأثیر چشم‌گیر" فراهم نمی‌کند. اما، توصیه می‌شود واپایش‌های امنیت اطلاعات این "رخدادهای با فراوانی پایین/ با تأثیر چشم-گیر" را پوشش دهد. محاسبه زیان مورد انتظار متوسط می‌تواند نتایج بهتری نسبت به ALE داشته باشد.	بله کاهش مخاطره مستقیماً سطوح زیان مورد انتظار را به‌وجود می‌آورد	خیر گواهی به‌طور مستقیم مخاطره پایین‌تر و نرخ زیان مورد انتظار را ایجاد نمی‌کند	بله افزایش مخارج در مقابله با مخاطره عملیاتی سازمان تا جد زیادی مخاطرات و زیان‌هایی مورد انتظار را کاهش می‌دهد.	بله واپایش‌ها را می‌توان مستقیماً برای کاهش مخاطره به‌کار برد
چ	حفظ شهرت و قیمت سهم از طریق توانایی کار تجاری در تمایز	بله مخاطرات احتمالاً اثرات برجسته‌ای را	بله گواهی می‌تواند شهرت را بهبود	بله افزایش مخارج در مقابله با مخاطره	خیر واپایش‌ها به‌طور مستقیم در حفظ

مرجع	اهداف تجاری	تصمیمات هزینه‌ای			
		هزینه‌های کاهش مخاطره	هزینه‌های گواهی	هزینه‌های سازمانی مدیریت مخاطره	هزینه‌های واپایش
	گذاشتن بر اعتماد ایجاد می‌شود مثل تصدیق کردن استانداردها و کاهش مخاطراتی که در صورت وقوع بیشتر شهرت را تحت تأثیر قرار می‌دهد	به وجود می‌آورد که می‌توان آن‌ها را کاهش داد	بخشد	عملیاتی سازمان تا حد زیادی می‌تواند شهرت را بخصوص برای کارمندان بالقوه بهبود بخشد	قیمت سهم مشارکت ندارند. این امر بیشتر با ISM و بلوغ ISMS سروکار دارد.
ح	کمینه‌سازی هزینه‌های عملیاتی مورد انتظار مدیریت مخاطره و امنیت اطلاعاتی، مثلاً از طریق بهبود کارایی	خیر کاهش مخاطره باعث نمی‌شود عملیات‌ها کارآمدتر باشند	خیر از گواهی انتظار هزینه عملیاتی پایین‌تر وجود ندارد	خیر- با افزایش مقدار صرف شده در مدیریت مخاطره نمی‌توان انتظار داشت که کارآمدی مستقیماً بهبود یابد	خیر واپایش‌ها به‌طور مستقیم در بهبود کارآمدی مرتبط با مدیریت مخاطره مشارکت ندارند. این موضوع بیشتر با ISM و کمال ISMS شامل آگاهی ، سنجش‌ها و حسابرس‌ها و غیره سروکار دارند
خ	ارائه بیمه با تکمیل و صحت اطلاعات مربوط به مخاطره و گزارشگری نظارت به شناسایی	بله افزایش سرمایه‌گذاری از بیمه به شناسایی بر طرف سازی ناکارآمد مخاطره و ایجاد بهبود متعاقب آن تمایل دارد	بله گواهی باعث افزایش بیمه فرایند می‌شود.	بله افزایش فقره افزایش عملکرد بیمه را امکان‌پذیر خواهد ساخت	خیر واپایش‌ها به‌طور مستقیم در مقابله با مخاطره و نظارت شرکت نمی‌کنند. و بیشتر با ISM و کمالISMS شامل آگاهی ، سنجش‌ها و حسابرس‌ها و غیره سروکار دارند.
د	حفاظت از کارکنان در برابر مسئولیت شخصی مثل عملکرد به دلیل جدیت در اجتناب از	بله اگر اعضای هیئت مدیره اعمال کار باشند	بله ممکن است اعضای هیئت مدیره بتوانند	بله اگر اعضای هیئت مدیره احتمال کار باشند در این صورت	بله واپایش نقش‌ها و مسئولیت برای امنیت اطلاعات

مرجع	اهداف تجاری	تصمیمات هزینه‌ای			
		هزینه‌های کاهش مخاطره	هزینه‌های گواهی	هزینه‌های سازمانی مدیریت مخاطره	هزینه‌های واپایش
	مسئولیت عضو هیئت مدیره	در این صورت سرمایه‌گذاری در کاهش مخاطره کافی نخواهد بود	هزینه‌های گواهی را به موجب پیشکارشان و از طریق کسب گواهی خارجی کسب کنند	سرمایه‌گذاری در کاهش مخاطره کافی نخواهد بود	
ذ	تأمین انتظارات جامعه به‌عنوان یک زیرساخت و تأمین کننده خدمات از طریق حفاظت اطلاعات آن‌ها	بله مخاطرات را می‌توان برای اطلاعات مشتری کاهش داد	بله گواهی را می‌توان برای بهبود حفاظت از اطلاعات مشتری به‌کار برد	خیر افزایش مخارج در مدیریت مخاطره مستقیماً به بهبود حفاظت از اطلاعات مشتری منجر نمی‌شود	خیر واپایش‌ها به‌طور مستقیم در انتظارات جامعه سهمی ندارند این بیشتر با ISM در کمالISMS شامل آگاهی ، سنجش‌ها و حسابرس‌ها و غیره سروکار دارد تا بازخورد را برای جامعه تأمین کند
ر	فراهم کردن فرصت‌های کاری برای جامعه	بله صرف هزینه برای کاهش مخاطره فرصت‌های کاری را برای کسانی که کار کاهش مخاطره را انجام می‌دهند فراهم می‌کند	خیر گواهی مستقیماً به فرصت‌های کاری منجر نمی‌شود	بله افزایش مخارج در مدیریت مخاطره سازمان فرصت‌های کاری بیشتری ایجاد می‌کند	خیر واپایش‌ها به‌طور مستقیم در فرصت‌های کاری نقشی ندارند این امر بیشتر با ISM و بلوغ ISMS شامل آگاهی سنجش‌ها و ممیزی‌ها و غیره سروکار دارد.
ز	اجتناب از الزامات برای مخاطره و حسابرسی سرمایه و وظیفه مراقبت اضافی از طریق عملکرد در قالب	بله کاهش یک ابزار اجتناب از مخاطره و حسابرسی سرمایه است	خیر گواهی مستقیماً به کاهش مخاطره و تخصیص حسابرسی سرمایه	خیر افزایش مخارج برای مدیریت مخاطره سازمان ب طور مستقیم به کاهش	خیر واپایش‌ها به‌طور مستقیم از مخاطره و تخصیص ممیزی سرمایه اجتناب

مرجع	اهداف تجاری	تصمیمات هزینه‌ای			
		هزینه‌های کاهش مخاطره	هزینه‌های گواهی	هزینه‌های سازمانی مدیریت مخاطره	هزینه‌های واپایش
	پارامترهای پذیرفته شده		منجر نمی‌شود	مخاطره و حسابرسی سرمایه منجر نمی‌شود	نمی‌کند (مگر آن-که واپایش‌ها ناقص باشند)
ژ	اجتناب از تاثیرات بر طرف‌های خارجی مانند زیرساخت و تأمین‌کنندگان خدمات	بله کاهش مخاطره تا حدی مخاطره تأثیر بر طرف‌های خارجی و زیرساخت و تأمین‌کنندگان خدمات را کاهش می‌دهد	خیر گواهی مستقیماً به کاهش اثرات برای طرف‌های خارجی منجر نمی‌شود	خیر افزایش مخارج برای مدیریت مخاطره سازمان مستقیماً به کاهش مخاطره طرف‌های خارجی ختم نمی‌شود	بله ممکن است واپایش‌ها به‌طور مستقیم از تاثیرات اجتناب کنند
س	سامانه‌هایی برای مدیریت و اشاعه خط مشی‌ها، روال‌های امنیتی	بله احتمال کاهش مخاطرات خطاهای انسانی را دارد	خیر قسمتی از دامنه ممیزی گواهی و مشارکت خواهد نمود.	خیر افزایشی در هزینه-های مدیریت مخاطره سازمان وجود ندارد.	خیر واپایش‌ها به‌طور مستقیم در آموزش نقشی ندارند این امر بیشتر با ISM و بلوغ ISMS شامل آگاهی سنجش‌ها و ممیزی‌ها و غیره سروکار دارد.
ش	سامانه‌هایی برای مدیریت و اشاعه سامانه‌های مدیریت برای واپایش IDهای کاربران/ حقوق دسترسی / موافقت‌ها و غیره برای کاربرد سامانه‌ها	بله تمایل به کاهش مخاطرات ضرر اطمینان بخش بودن و یکپارچگی و احتمال افزایش هزینه‌های جابجایی و هزینه‌های راه‌حل‌های فنی	خیر ممکن است بخشی از گواهی دامنه کاربرد حسابرس باشد	خیر هیچ افزایشی در هزینه‌های مدیریت مخاطره سازمان وجود ندارد	بله واپایش‌های مرتبط با این موضوع به‌کار می‌رود
ص	آسیب‌پذیری و سامانه‌های مدیریت تغییر برای به حفظ بروز رسانی با	تمایل به کاهش مخاطرات ضرر اطمینان بخشی و یکپارچگی احتمال	خیر ممکن است بخشی از گواهی دامنه کاربرد	خیر هیچ افزایشی در هزینه‌های مدیریت مخاطره سازمان	بله واپایش‌های مرتبط با این موضوع به کار می‌رود

مرجع	اهداف تجاری	تصمیمات هزینه‌ای			
		هزینه‌های کاهش مخاطره	هزینه‌های گواهی	هزینه‌های سازمانی مدیریت مخاطره	هزینه‌های واپایش
	بخش‌های امنیتی	افزایش هزینه‌های جابجایی و هزینه‌های راه‌حل‌های فنی	حسابرس می‌باشد	وجود ندارد	
ض	رخدادها با یک ارزش کافی تقریبی جهت توجیه نسل ISMS که به صرفه جویی کلی منجر خواهد شد برآوردهای فراهم شده به نحو رضایت بخشی محافظه‌کارانه بوده و برای چالش مدیریت بقا منطقی بوده، کاهش هزینه‌های رخداد به‌تنهایی به‌طور خاص بیشتر رضایت‌بخش خواهد بود تا توجیه هزینه ISMS در غیر این صورت آن‌ها کل مورد کسب‌وکار را نمی‌سازند	بله اگر رخدادها به فرایندهای مدیریت مخاطره اضافه شوند باعث افزایش پیچیدگی خواهد شد ولی ارزشیابی دقیق‌تری را تأمین خواهد کرد	خیر ممکن است بخشی از گواهی دامنه کاربرد حسابرسی باشد	بله ممکن است هزینه مدیریت مخاطره سازمان را افزایش دهد	بله واپایش‌های مرتبط با این موضوع را به‌کار می‌برند
ط	پرداختن به مخاطرات امنیت اطلاعات و واپایش‌های برای بازار، قانونی[1] یا دلایل تنظیم	بله توصیه می‌شود این مورد قسمت عمده از ساماندهی مخاطره باشد	بله بخش از گواهی	بله ممکن است مخاطره سازمان را افزایش دهد	بله واپایش‌های انطباق به‌کار می‌روند

1- Legal

پیوست پ
(اطلاعاتی)
مدل‌های اقتصادی مناسب برای امنیت اطلاعات

پ-۱ اطلاعات کلی

مدل‌های محاسبه متعددی وجود دارند که در اقتصاد به‌کار می‌روند و می‌توان آن‌ها را همانند سایر مدل‌ها در چارچوب امنیت اطلاعات به‌کار برد. تنها مدل‌های بسیار عمومی در این پیوست فهرست شده‌اند.

ممکن است شناسایی مفاهیم دقیق اقتصادی پیاده‌سازی فرایندها، روش‌ها یا معیارهای فنی پیاده‌سازی امنیت اطلاعات دشوار باشد. بنابراین توصیه می‌شود نتایج محاسبات در گستره‌هایی با استفاده از مقادیر نسبتا بیشینه و کمینه ارائه گردد. این در مدل‌ها گنجانده نمی‌شود و با استفاده از یک مدل، اما با مقادیر یا هزینه‌های متفاوت انجام می‌شود.

پ-۲ مدل مقادیر پایه

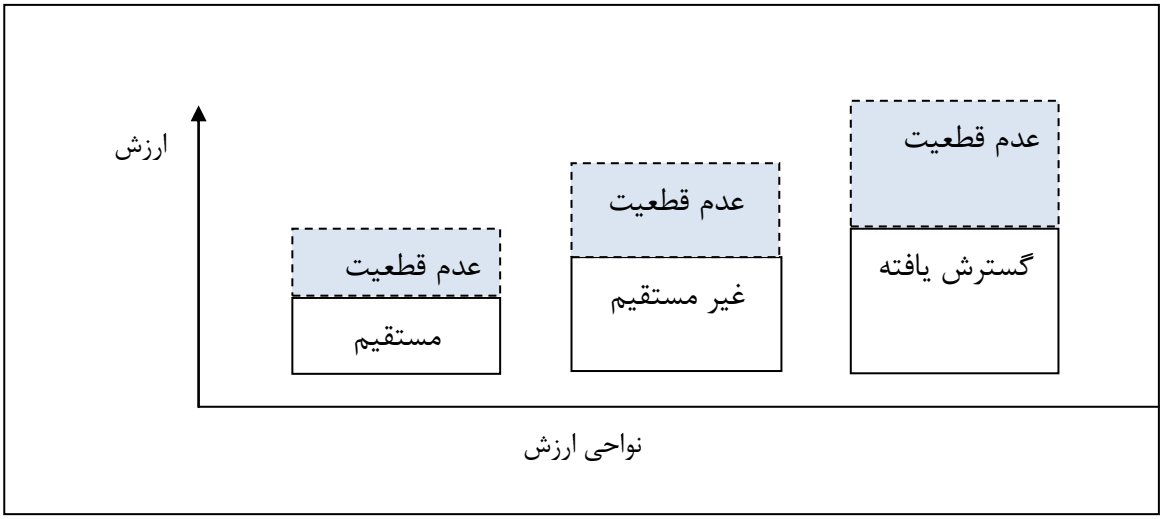
اصل ۱ مدل مقدار پایه هم برای مقادیر مثبت (محصول) و مقادیر منفی (هزینه‌ها) به‌کار می‌رود و توصیه می‌شود در اتصال منفی به مثبت و ترازنامه استفاده شود که در جدول برای تکمیل مجموعه‌ای از مراحل روش جهت ارزشیابی و ارائه نتایج ارائه گردیده است.

اصل BVM1 مبتنی بر سه بخش با مشخصه‌های متفاوت است:

مقادیر مستقیم، مقادیر اقتصادی مستقیم مانند ضرر مواد، یا سرمایه‌گذاری مستقیم مبتنی بر وقوع را پوشش می‌دهد که می‌تواند مجهول یا معلوم باشد. مقادیر در این ناحیه دقیق‌تر هستند.

مقادیر غیرمستقیم تعمیم‌هایی برای مقادیر مستقیم بوده و مقادیر ملموس‌تر از دسته رفته یا به‌دست‌آمده و مقادیر اضافی را نشان می‌دهد. مقادیر غیرمستقیم عدم قطعیت بیشتری داشته و می‌توانند درون محدوده-هایی نوشته شوند. آن‌ها یک ارزشیابی از مقادیری مانند خروجی ضایع‌شده، افزایش رسیدگی و غیره هستند.

مقادیر توسعه یافته، آن مقادیری هستند که از مقادیر مستقیم و غیرمستقیم تاثیر می‌پذیرند و می‌توانند کاملا بااهمیت باشند. مقادیر توسعه یافته گستره بزرگ‌تری داشته و باید با استفاده از یک مبنای مشابه مانند مقادیر مستقیم و غیرمستقیم محاسبه شوند، اما از عوامل دیگر مانند اثر بر جامعه و یا سازمان به‌طورکلی، یا قیمت سهم در صورت ارتباط و غیره تاثیر می‌پذیرند. اغلب اوقات پرداختن تعیین کمیت مقادیر توسعه یافته اقلامی مانند علامت تجاری، شهرت و غیره دشوار است. (توجه داشته باشید اغلب اوقات مقادیر توسعه یافته احتمالا منفی هستند اما ممکن است در نتیجه کاربرد امنیت اطلاعات مثبت نیز باشند.)



شکل پ-۱ مدل اصل مقدار مبنا

پ-۳ مدل منفی و مثبت

یک رویکرد برای تبدیل مقادیر منفی به مقادیر مثبت بر اساس سوالات متفاوت و جایگزین

- درصورتی‌که فعالیتی انجام نشود، مقادیر منفی چه خواهند بود؟
- درصورتی‌که فعالیتی انجام نشود، مقادیر مثبت چه خواهند بود؟
- درصورتی‌که فعالیتی انجام شود، مقادیر منفی چه خواهند بود؟
- درصورتی‌که فعالیتی انجام شود، مقادیر مثبت چه خواهند بود؟

یادآوری – مقادیر به‌کار رفته در مدل همچون هزینه‌ها می‌توانند مثبت باشند.

پاسخ به این سوالات به همراه ترکیب با اصل مدل ارزش مبنا در شکل پ-۱ ، صفحه ترازی را با چهار مربع نتیجه می‌دهد که در شکل پ-۲ نمایش داده شده است.

مقدار مثبت غیرفعال	مقدار مثبت فعال
مقدار منفی غیرفعال[1]	مقدار منفی فعال

شکل پ-۲ مدل منفی به مثبت

استفاده از مدل پوشش همه جنبه‌ها را تضمین خواهد کرد. اما مقادیر تکراری مربوط به فعالیت مشابه همچنان وجود دارد. این را می‌توان با استفاده از یک جدول تراز ساده همانند جدول پ-۱ساماندهی کرد.

با مراجعه به جدول پ-۱ می‌توان فهمید در بعضی موارد مقدار A_1 مشابه مقدار D_2 بوده بنابراین مقدار / هزینه منفی در هنگام مقایسه خالص برای دو ردیف (۱ و ۲) به مثبت تبدیل می‌شود.

1- Non-active

(در صورتی‌که یک فعالیت پیچیده باشد، ردیف‌های بیشتری را می‌توان به‌کار برد اما توصیه می‌شود خلاصه بین وضعیت فعلی باشد (فعالیت احتمالی انجام نشده) و در این هنگام فعالیت کاملا پیاده‌سازی/اجرا شده است).

جدول پ-۱–تعادل برای مقادیر خالص

	مبنا	فعالیت	مقدار مثبت فعالیت انجام شده	مقدار مثبت فعالیت انجام نشده	مقدار منفی فعالیت انجام شده	مقدار منفی فعالیت انجام نشده	خالص
مرجع			الف	ب	پ	ت	
۱	فعالیت احتمالی برای تغییر موقعیت فعلی	فعالیت x انجام شده	مقدار	غیرقابل کاربرد	هزینه	غیرقابل کاربرد	۱A – ۱B
۲	فعالیت احتمالی انجام نشده	فعالیت x انجام نشده	غیرقابل کاربرد	مقدار	غیرقابل کاربرد	هزینه	۲B – ۲D

پ-۴ سرمایه‌گذاری تراز عمومی برای هزینه حفاظت در مقایسه با تئوری مقدار

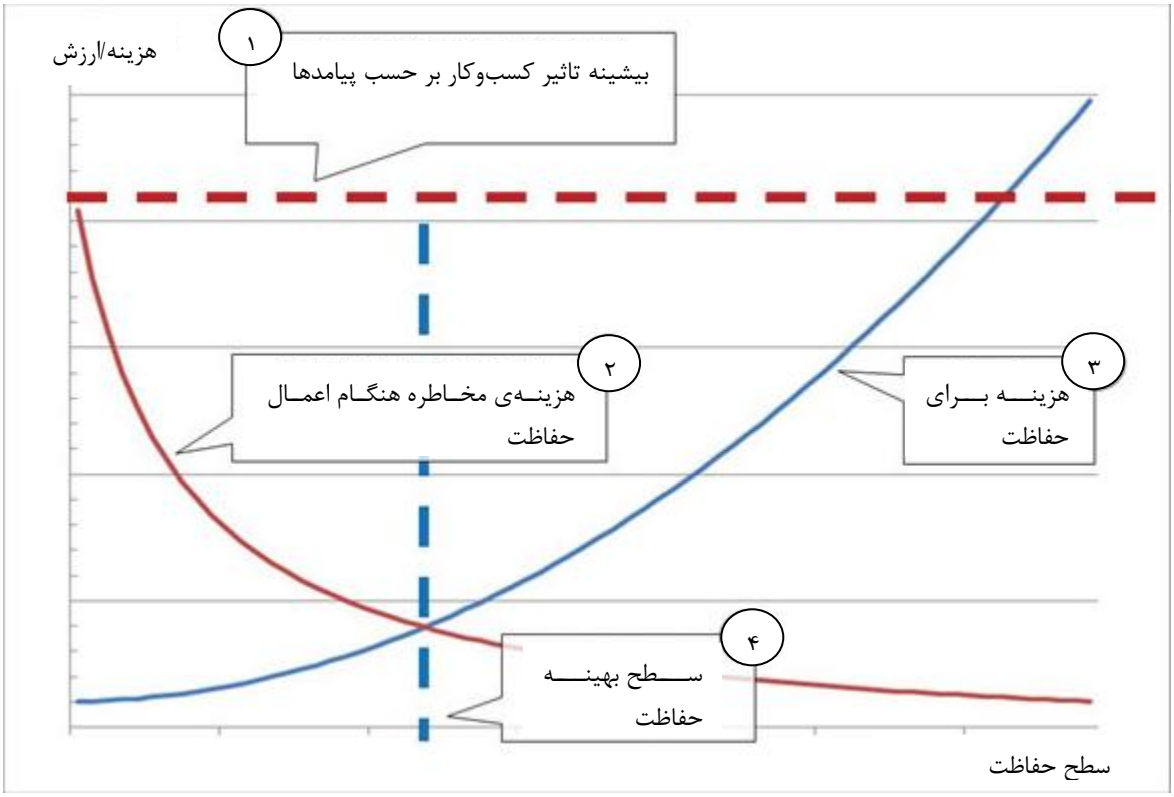
در این تئوری می‌توان به یک نقطه تراز بهینه از طریق کاربرد هزینه‌های حفاظت تدریجی برای مقدار دست یافت. نقطه بهینه بین هزینه‌های حفاظت و مقدار قرار دارد در این هنگام کاهش مخاطره بر مقداری تاثیر داشت که از هزینه حفاظت کمتر باشد. عوامل اصلی نظر به شرح زیر هستند:

الف) آگاهی از مقدار (کدام ثابت است)

ب) هزینه مشخص شده برای حفاظت (کدام یک در ارتباط با فعالیت‌ها افزایش خواهد یافت)

پ) کاهش مخاطره در ارتباط با کاربرد حفاظت (کدام یک براساس مقدار بوده و نحوه اثربخشی حفاظت)

اغلب اوقات مقدار و هزینه‌های حفاظت را می‌توان تعیین کرد اما کاهش مخاطره یک تخمین است.



شکل پ-۳ نظریه تراز بهینه بین هزینه حفاظت و مقدار

پ-۵ محاسبه سرمایه‌گذاری عمومی – محاسبه منفعت هزینه

اغلب اوقات تحلیل هزینه – منفعت به‌وسیله دولت‌ها و سایرین مانند تجارت‌ها جهت ارزشیابی ضرورت دخالت ارائه شده به‌کار می‌رود. این یک تحلیل از اثربخشی هزینه جایگزین‌های متفاوت است تا ببینیم آیا منافع بر هزینه‌ها غلبه می‌کند یا خیر آیا اصل ارزش دخالت دارد) ، و این برتری به چه میزان است (کدام دخالت انتخاب شود)

هدف این کار تخمین اثربخشی دخالت‌ها در ارتباط با یکدیگر و وضع موجود است. اثربخشی Pareto برای دستیابی به بهترین نتایج به‌کار می‌رود.

فهرست مراحل زیر تحلیل عمومی هزینه – منفعت را تشکیل می‌دهند.

الف) استقرار پروژه‌ها / برنامه‌های جایگزین

ب) گردآوری فهرستی از متصدیان اصلی

پ) انتخاب سنجش و جمع‌آوری همه هزینه‌ها و اجزای منافع

ت) پیش‌بینی نتیجه هزینه‌ها و منافع در طول دوره زمانی پروژه

ث) قرار دادن اثرات هزینه‌ها و منافع به صورت عدد در پول

ج) اعمال نرخ تخفیف (می‌تواند نرخ مالی داخلی باشد)[1]
ح) محاسبه ارزش فعلی خالص گزینه‌های پروژه
خ) تحلیل حساسیت
د) توصیه

۱ - اغلب به وسیله انبار مالی تامین می گردد.

پیوست ت

(اطلاعاتی)

مثال‌های محاسبه موارد کسب‌وکار

ت-۱ مثال محاسبه مورد کسب‌وکار سازمانی (مرجع الف)

توصیف: کسب‌وکار بیشتر و بیشتر با موارد مرتبط با مشتری مواجه می‌گردد که نیازمند هم‌ترازی با استاندارد ISO/IEC 27001، می‌باشد. واحد بازاریابی تقاضا نموده است که توصیه می‌شود سازمان یک گواهی استاندارد ملی ایران شماره ۲۷۰۰۱ : سال ۱۳۸۷، را در نظر بگیرد. وظیفه CISO محاسبه یک مورد کسب‌وکار اقتصادی برای پیاده‌سازی یک ISMS با توجه به استاندارد ISO/IEC 27001 و همین‌طور لحاظ نمودن ورودی کافی جهت تشویق مدیران ارشد به آغاز پروژه پیاده‌سازی، می‌باشد (همان‌طور که در استاندارد ISO/IEC 27003 [۳] شرح داده شد).

محتوا: توصیه می‌شود کل سازمان گواهی را اخذ کند.

یک مورد کسب‌وکار برای یک ISMS طی یک مدت طولانی بر روی سازمان موثر خواهد بود؛ این امر باید در محاسبات در نظر گرفته شود. این اتفاق به این صورت می‌تواند صورت پذیرد که یک دوره زمانی مفروض در نظر گرفته شده و مقادیر و هزینه‌ها برای این دوره زمانی محاسبه شوند یا با بیان تصمیم برای سرمایه‌گذاری‌ها در زمان اخذ تصمیم (برای مثال یک سال) و تراز نمودن این مقادیر به مدت یک سال و درنتیجه عدم منظور نمودن آن‌ها، تسهیل گردد. مورد دوم به‌عنوان یک نقطه آغازین برای محاسبه این مورد کسب‌وکار انتخاب شده و سپس یک گستره بیشینه و کمینه برای تاکید بر روی y غیرقطعی مورد استفاده قرار می‌گیرد. بعد زمانی نیز در صورت نیاز لحاظ می‌گردد.

مرجع	عامل‌ها	مبنا	ارزش مرتبط			هزینه مرتبط		
		(گستره)	مستقیم	غیرمستقیم	افزوده	مستقیم	غیرمستقیم	افزوده
الف	گردش فروش سالیانه:	۱۰۰ میلیون دلار	x	۱۰۰میلیون دلار * ۳٪ = ۳ میلیون دلار	x	x	x	x
ب	افزایش فروش احتمالی با گواهی سالیانه:	۳٪ (۱٪-۵٪)	x	x	x	x	x	x
پ	سرمایه‌گذاری مجاز است:	۱۰ سال	x	x	x	x	x	x
ت	هزینه پروژه پیاده‌سازی ISMS:	(±۲۰٪)	x	x	x	۰.۵ میلیون دلار	x	x
ث	هزینه گواهی به‌عنوان	n/a	x	x	x	۰.۳	x	x

مرجع	عامل‌ها	مبنا	ارزش مرتبط			هزینه مرتبط		
	بخشی از پروژه:					میلیون دلار		
ج	افت بهره‌وری داخلی طی پروژه	(±٪۲۰)	x	x	x	x	تخمین زده‌شده*	x
چ	ISMS واپایش‌های هزینه پیاده‌سازی برای گواهی طی پروژه:	(±٪۲۰)	x	x	x	۰.۳ میلیون دلار	۰.۲ میلیون دلار	x
ح	هزینه اجرای سالیانه ISMS:	x	x	x	x	۰.۱ میلیون دلار	x	X
خ	افزایش سالیانه بهره‌وری داخلی	تخمین زده نشده*	x	تخمین زده نشده*	x	x	x	x
د	ارزش ممیزی‌های کاهش‌یافته *	تخمین زده نشده*	تخمین زده نشده *	تخمین زده نشده*	x	x	x	x
ذ	ارزش مخاطره کاهش‌یافته*	تخمین زده نشده*	تخمین زده نشده *	تخمین زده نشده*	تخمین زده نشده*	x	x	x
ر	ارزش انطباق *	تخمین زده نشده*	تخمین زده نشده *	تخمین زده نشده*	تخمین زده نشده*	x	x	x
ز	ارزش تصویر/ علامت تجاری*	تخمین زده نشده*	x	x	تخمین زده نشده*	x	x	x
ژ	هزینه کلی گواهی به‌صورت سالیانه (به‌جز مهر و موم‌های اولیه)	تخمین زده نشده*	x	x	x	تخمین زده نشده*	x	x

*این هزینه و یا دیگر ارزش‌ها را نیز می‌توان به‌عنوان بخشی از مورد کسب‌وکار برآورد نموده و در محاسبات لحاظ نمود اگر این‌گونه به نظر برسد که آن‌ها اثری بر روی عملی نمودن تصمیم خواهند داشت.

یادآوری- شکل‌های محاسبه تنها به صورت مصور بوده و به هیچ‌گونه موقعیت واقعی مرتبط نیستند.

محاسبه اولیه برای نتیجه‌گیری مبتنی بر ارزش‌های برآوردشده بدون استفاده از یک گستره می‌باشد.

نتیجه‌گیری ۱ مبنا:

طی سال پس از گواهی، ارزش افزوده برابر است با: ۳.۰ میلیون دلار

هزینه‌ها به‌طورخلاصه برابر است با: ۱.۴- میلیون دلار

حاصل‌جمع: ۱.۶+ میلیون دلار

نتیجه‌گیری ۲ گستره:

محاسبه دوم برای نتیجه‌گیری بر مبنای ارزش‌های استفاده شده در گستره‌ی ارزش‌های بیشینه(Max) و کمینه (Min). ارزش‌های بیشینه نشان دهنده بالاترین ارزش و پایین‌ترین هزینه و ارزش‌های کمینه نشان-دهنده پایین‌ترین ارزش‌ها و بالاترین هزینه‌ها (لطفا برای تغییرات به دلیل عدم قطعیت‌ها به جدول بالا مراجعه شود).

بیشینه: طی سال پس از گواهی، حداکثر ارزش‌افزوده برابر است با: ۵.۰ میلیون دلار

هزینه‌ها از محاسبه ۱ تا ۲۰ درصد کاهش می‌یابند: ۱.۴- میلیون دلار * ۸۰٪ = ۱.۱۲- میلیون دلار

حاصل جمع: ۳.۸۸+ میلیون دلار

کمینه: طی سال پس از گواهی، حداکثر ارزش‌افزوده برابر است با: ۱.۰ میلیون دلار

هزینه‌ها از محاسبه ۱ تا ۲۰ درصد کاهش می‌یابند: ۱.۴- میلیون دلار * ۱۲۰٪ = ۲.۳۵- میلیون دلار

حاصل جمع: ۱.۳۵- میلیون دلار

نتیجه‌گیری ۲ نشان می‌دهد که علیرغم یک سناریوی اقتصادی مثبت‌تر، ممکن است موقعیتی وجود داشته باشد که در آن مورد کسب‌وکار برحسب تصمیم مبتنی بر اقتصاد، پیامدی منفی دارد. این امر نشان می‌دهد که تحلیل بیشتری ممکن است مورد نیاز باشد. احتمال محاسبه "کمینه" توصیه می‌شود مجددا محاسبه گردد و شاید افزودن برآوردهای بیشتر به عوامل موجود در جدول برای دیدن ارزش‌ها و هزینه‌های بیشتر، ممکن است نتیجه اقتصادی منفی را در محاسبه تغییر دهد.

توصیه می‌شود تحلیل احتمال نقطه آغازین باشد همان‌طور که این امر ممکن است شواهد آشکاری را نشان دهد که احتمال کمی وجود دارد که توصیه می‌شود در مراحل بعدی لحاظ گردد (به‌عنوان دلیلی برای ارائه محاسبه ۱ به‌عنوان مبنایی برای مورد کسب‌وکار).

در جایی که سازمان دارای گواهی نیست، چنین تحلیلی می‌تواند یک سناریوی جایگزین باشد که از سوی واحد فروش و بازاریابی فراهم شده است و نشان می‌دهد که یک کاهش احتمالی در فروش (تا ۱۵ درصد) طی یک دوره سه‌ساله وجود دارد. این امر مربوط به بخش مشتری مداری است که در این مرحله هم‌ترازی با استاندارد ملی ایران شماره ۲۷۰۰۱ : سال ۱۳۸۷ [۱] را طلب می‌کند. در مقایسه محاسبه ۱، کاهش ۱۵ درصدی یک مقدار بالا بوده (همان‌طور که تاثیر منفی همان ارزش مثبت برای تشویق مورد کسب‌وکار می‌باشد) و نشان می‌دهد که تحلیل بیشتر منجر به تغییر عمده‌ای نخواهد شد.

مورد کسب‌وکار را می‌توان همچون محاسبه ۱ عرضه نمود که دارای سناریوی جایگزین از تحلیل احتمال می‌باشد.

ت-۲ مثال محاسبه جزیی مورد کسب‌وکار سازمانی (مرجع ب)

مورد: این مثال مورد کسب‌وکار به یک دارایی خاص مربوط می‌باشد که برای آن واپایش‌های متعدد امنیت اطلاعاتی را می‌توان اعمال نمود. بنابراین، این مثال یک مورد کسب‌وکار محدود است. هزینه‌های این واپایش‌ها در مثال لحاظ نمی‌شوند، در عوض، هزینه‌های عدم اعمال واپایش‌ها محاسبه می‌شوند که می‌توان آن‌ها را در مراحل بعدی به‌عنوان یک ارزش مثبت در نظر گرفت تا هزینه‌های واپایش را در مرحله دوم خنثی نمود. تصمیم ISM برای مورد کسب‌وکار همان رفتن به مرحله بعد و تعیین واپایش‌ها و هزینه‌های واپایش می‌باشد.

دارایی اطلاعاتی

سازمان دارای دادگان از ۲۵۰.۰۰۰ مشتری می‌باشد. اطلاعات موجود در دادگان شامل اطلاعات فردی قابل شناسایی برای هر مراجعه کننده، جزئیات کارت اعتبار شخصی و اطلاعات سوابق تراکنش‌های صورت گرفته بین مشتری و سازمان طی ۱۰ سال اخیر، می‌باشد.

مخاطرات و هزینه‌های مرتبط

مخاطرات مربوط به دارایی اطلاعاتی باید در نظر گرفته شده و از لحاظ محرمانگی، یکپارچگی و دسترس‌پذیری ارزشیابی شوند:

عامل CIA	شرح مخاطره	هزینه برای سازمان
محرمانگی	دادگان از سوی افراد غیرمجاز قابل دسترسی بوده و از کل اطلاعات نسخه‌برداری می‌شود. حال، اطلاعات جهت سو استفاده از هویت مشتریان سازمان و انجام تراکنش‌های غیرمجاز با استفاده از اطلاعات شخصی و اطلاعات کارت اعتباری آن‌ها، به‌کار گرفته می‌شود.	به هر فرد باید اطلاع‌رسانی شود که اطلاعات شخصی وی با مخاطره افشا مواجه است (۲۵دلار برای هر مشتری) (تعداد مشتریان در یک نقض قانون به میزان ۱۰۰۰ نفر برآورد می‌گردد) افشای اطلاعات مشتری منجر به قانون‌شکنی می‌گردد (۵۰۰هزار دلار جریمه مجزا) سازمان باید منابع را مجددا هدایت کند تا دلایل قانون‌شکنی را تعیین نموده، به بازپرسی‌های اجرای احکام و اصلاح سامانه اطلاعاتی جهت جلوگیری از قانون‌شکنی‌های آتی کمک کند (۲۵۰هزار دلار برای یک دوره معین)
یکپارچگی	مشتری یک سازمان وارد یک تراکنش آنلاین می‌شود و طی این تراکنش، اطلاعات/جزییات شخصی مشتری سازمان دیگر نمایش داده می‌شود.	هر تراکنش باید بازبینی گردد تا تائید شود آیا اطلاعات صحیح وجود دارد یا خیر (۲۵ دلار برای هر تراکنش) (تعداد مشتریان در یک نقض قانون به میزان ۱۰۰۰ نفر برآورد می‌گردد) نمایش غیرمجاز اطلاعات مشتری منجر به نقض قانون می‌گردد (۵۰۰هزار دلار جریمه به‌طور مجزا) افت کسب‌وکار آتی چراکه مشتریان تجارت خود را به رقبا می‌سپارند (۱۰۰دلار به ازای از دست دادن هر مشتری) (برآورد ۴۰٪ از مشتریان در یک قانون‌شکنی (۱۰۰۰))

عامل CIA	شرح مخاطره	هزینه برای سازمان
دسترس‌پذیری	دادگان خراب شده و هیچ اطلاعاتی در دسترس کاربران مجاز نیست	در راستای تعیین دلیل افت داده‌ها، سازمان باید منابع را مجددا هدایت کند و عهده‌دار واپایش‌های مخفف جهت بازگرداندن دسترسی باشد (شامل تماس با مشاورین) (۵۰۰۰ دلار در هر ساعت) (برآورد شده در ۳۰۰ ساعت) بهره‌وری صفر کارکنان، به دلیل آنکه هیچ تراکنشی برای انجام وجود ندارد (۱۰۰هزار دلار در هر ساعت) (برآورد شده در ۱۰ ساعت) افت کسب‌وکار فعلی ازآن‌جائی‌که مشتریان قادر به انجام تراکنش نیستند (۱۰۰ دلار به ازای ترک هر مشتری) (برآورد ۲۰ درصد مشتریان در یک قانون‌شکنی (۱۰۰۰))

در جدول زیر، حاصل جمع هزینه‌ها معرف ارزش هم‌ترازی هزینه‌های واپایش در مرحله بعدی است:

CIA	مربوط به مشتری	وضع قانون	توقف کسب‌وکار	تخصیص منابع	حاصل جمع
محرمانگی	$۲۵*۱۰۰۰ =$۲۵۰۰۰	$۵۰۰۰۰۰	x	$۲۵۰۰۰۰	$۷۷۵۰۰۰
یکپارچگی	$۲۵*۱۰۰۰۰ =$۲۵۰۰۰۰ $۱۰۰*(۴۰٪*۱۰۰۰) =$۴۰۰۰۰	$۵۰۰۰۰۰	x		$۷۹۰۰۰۰
دسترس‌پذیری	$۱۰۰*(۲۰٪*۱۰۰۰) =$۲۰۰۰۰	x	$۱۰۰۰۰۰*۱۰ =$۱۰۰۰۰۰۰	$۵۰۰۰*۳۰۰ =$۱۵۰۰۰۰۰	۲۵۲۰۰۰۰ $
حاصل جمع	$۳۳۵۰۰۰	$۱۰۰۰۰۰۰	$۱۰۰۰۰۰۰	$۱۷۵۰۰۰۰	۴۰۸۵۰۰۰ $

ت-۳ مثال مورد دارایی/واپایش (مرجع ب)

مورد: اعمال یک فعالیت آگاهی امنیت اطلاعاتی کاربر جهت استفاده از اینترنت. این مثال مورد کسب‌وکار به یک فعالیت خاص و تعداد بسیار محدودی از واپایش‌ها مربوط می‌باشد. حتی اگر واپایش‌ها در سرتاسر سازمان اعمال شوند، به دلیل وجود تعداد کمی از واپایش‌ها، این نمونه همچنان به‌عنوان یک مورد کسب‌وکار محدود در نظر گرفته می‌شود. تصمیم ISM برای مورد کسب‌وکار همان شروع فعالیت می‌باشد.

داده‌های اولیه:

تعداد کاربران:	۱۰۰۰
هزینه سالیانه رخدادهای مرتبط با اینترنت:	۱۰۰هزار دلار
اثر آموزش در راستای کاهش رخدادها:	۷۰درصد
هزینه مواد آموزشی:	۱۰هزار دلار
هزینه زمان درونی در هر ساعت:	۵۰دلار

ساعات زمان آموزش:	۱
طول تاثیر برنامه آموزشی:	۳ سال
توصیه می‌شود محاسبه مورد برای:	۳ سال
تعداد جلسات آموزشی طی دوره:	۲ مرتبه

بر اساس مدل موجود در پ-۳، محاسبات زیر صورت گرفته و سپس یک تحلیل حساسیت لحاظ می‌شود:

فعالیت	ارزش مثبت	ارزش/هزینه منفی	خالص
انجام آموزش اینترنت برای کاربران	$۲۱۰۰۰۰ (۳*۱۰۰۰۰۰*۷۰٪)	$۱۱۰۰۰۰ (۱۰۰۰۰+((۵۰*۱۰۰۰)*۲)	+$۱۰۰۰۰۰
عدم انجام آموزش اینترنت برای کاربران	$۱۰۰۰۰۰ (۵۰*۱۰۰۰*۲)	$۳۰۰۰۰۰ (۳*۱۰۰۰۰۰)	-$۲۵۰۰۰۰

نتیجه‌گیری: سود خالص اعمال فعالیت آموزشی طی سه سال برابر با ۱۰۰۰۰۰$+ است. ارزش منفی/هزینه‌های عدم انجام این فعالیت به‌طورخالص برابر با ۲۵۰۰۰۰$- است.

این محاسبه می‌تواند مبنایی را برای اخذ تصمیم جهت بر عهده گرفتن فعالیت و همچنین پیگیری میزان صحیح بودن محاسبه فراهم آورد. اگر تغییر معنی‌داری وجود دارد، اقدامات بیشتری را می‌توان تعیین و محاسبه نمود. (این مثال ممکن است پیچیده‌تر باشد از آنجائی که رخدادها را می‌توان بیشتر تعریف نمود. فرض بر این است که تمامی رخدادهایی که در این مثال به آن‌ها رجوع می‌شوند، به کاربر مرتبط می‌باشند.)

یک تحلیل حساسیت برای محاسبات این نکته را در نظر خواهد گرفت که تا چه حد اثر رخداد باید کاهش یابد. در راستای به‌دست آوردن نقطه سربه‌سر، این تحلیل با استفاده از جدول به‌طورمعکوس برروی فعالیت صورت گرفته انجام می‌پذیرد با تنظیم ارزش مثبت برابر با ارزش منفی/هزینه به‌طوریکه مقدار خالص برابر با صفر است. جدول زیر محاسبه مجدد مقدار مثبت را در راستای به‌دست آوردن درصد سربه‌سر کاهش رخداد نشان می‌دهد.

فعالیت	ارزش مثبت	ارزش منفی/هزینه	خالص
انجام آموزش اینترنت برای کاربران	$۱۱۰۰۰۰ (۳*۱۰۰۰۰۰*Y=$۱۱۰۰۰۰) Y=۱۱۰۰۰۰ / ۳ *۱۰۰۰۰۰(٪)=۳۷٪	$۱۱۰۰۰۰ (۱۰۰۰۰+((۵۰*۱۰۰۰)*۲)	$۰

تحلیل حساسیت نشان می‌دهد که تقریبا نیمی از کاهش رخدادهای تخمین زده باید به‌عنوان خروجی آموزش منظور گردد تا نقطه سربه‌سر به‌دست بیاید، یعنی پوشش هزینه‌ها.

کتاب‌نامه

[۱] استاندارد ملی ایران شماره ۲۷۰۰۱ : سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سامانه‌های مدیریت امنیت اطلاعات – الزامات

[۲] استاندارد ملی ایران شماره ۲۷۰۰۲ : سال ۱۳۸۷، فناوری اطلاعات – فنون امنیتی – سامانه‌های مدیریت امنیت اطلاعات – آیین کار مدیریت امنیت اطلاعات

[۳] استاندارد ملی ایران شماره ۲۷۰۰۳ : سال ۱۳۸۹، فناوری اطلاعات - فنون امنیتی - راهنمای اجرای سامانه مدیریت امنیت اطلاعات

[۴] استاندارد ملی ایران شماره ۲۷۰۳۱ : سال ۱۳۹۱، فناوری اطلاعات - فنون امنیتی - راهنماهایی برای آمادگی فناوری اطلاعات و ارتباطات به‌منظور تداوم کسب‌وکار

[۵] استاندارد ملی ایران شماره ۲۷۰۰۵ : سال ۱۳۹۲، فناوری اطلاعات – فنون امنیتی-مدیریت مخاطرات امنیت اطلاعات

[۶] استاندارد ملی ایران شماره ۲۷۰۰۶ : سال ۱۳۸۷، فناوری اطلاعات - فنون امنیتی -الزامات نهادهای ممیزی کننده و گواهی کننده سامانه‌های مدیریت امنیت اطلاعات

[۷] استاندارد ملی ایران شماره ۲۷۰۰۷ : سال ۱۳۹۱، فناوری اطلاعات -فنون امنیتی -راهنماهایی برای ممیزی سامانه‌های مدیریت امنیت اطلاعات

[۸] استاندارد ملی ایران شماره ۲۷۰۱۴ : سال ۱۳۹۲، فناوری اطلاعات -فنون امنیتی -حاکمیت امنیت اطلاعات

[9] ISO 31000:2009, *Risk management — Principles and guidelines*