مدل بلوغ مدیریت امنیت اطلاعات (O-ISM3)، نسخه ۲٫۰

مترجم:

محمد شروین جعفرزاده

مدل بلوغ مدیریت امنیت اطلاعات
(O-ISM3)، نسخه ۲٫۰

مترجم: محمد شروین جعفرزاده
طراحی جلد و صفحه‌آرایی: همتا بیداریان
ناشر: انتشارات آتی‌نگر
ناشر همکار: انتشارات وینا
چاپ اول، ۱۴۰۱
شمارگان: ۱۰۰ نسخه
قیمت: ۸۰۰,۰۰۰ ریال
شابک: ۳-۵۲-۷۵۷۱-۶۲۲-۹۷۸

ISBN: 978-622-7571-52-3

نشانی دفتر فروش: خیابان جمالزاده جنوبی، روبه‌روی کوچه رشتچی، پلاک ۱۴۴، واحد ۱
تلفن: ۸-۶۶۵۶۵۳۳۶ **نمابر:** ۶۶۵۶۵۳۳۷
www.ati-negar.com * info@ati-negar.com

سرشناسه: اپن گروپ، Open Group
مدل بلوغ مدیریت امنیت اطلاعات (O-ISM3)، نسخه ۲/۰/ [اپن گروپ]؛ مترجم محمدشروین جعفرزاده.
تهران: آتی‌نگر، وینا ۱۴۰۱
۱۹۴ ص.: مصور، جدول، نمودار.
ISBN: 978-622-7571-52-3
فیپا.
یادداشت: عنوان اصلی کتاب: .Open information security management maturity model (O-Ism3),Version 2.0,2017
یادداشت: واژه‌نامه.
موضوع: تکنولوژی اطلاعات -- تدابیر ایمنی-- تکنولوژی اطلاعات -- تدابیر ایمنی -- استانداردها-- حفاظت داده‌ها
موضوع: کامپیوترها -- ایمنی اطلاعات -- استانداردها-- شبکه‌های کامپیوتری -- تدابیر ایمنی -- استانداردها
موضوع: Data protection −Information technology -- Security measures – Standards −Information technology -- Security measures
موضوع: Computer networks -- Security measures -- Standards −Computer security – Standards
شناسه‌افزوده: جعفرزاده، محمد شروین ۱۳۶۰ -، مترجم
شناسه‌افزوده: بیداریان، همتا، ۱۳۶۱-، گرافیست
رده‌بندی کنگره T۵۸/۵
رده‌بندی دیویی ۳۰۳/۴۸۳۳
شماره کتابشناسی ملی ۸۹۲۳۵۴۰

31st January 2022

Mohammad Shervin Jafarzadeh
. No.203 - Block C1 - Mojtame Yass Complex - Seraj Ave
Farjam Ave - Tehranpars
Tehran – Iran
Phone: +98(912)2934303
Email: shervin1981@gmail.com

, Dear Mr. Jafarzadeh

Thank you for your request .

The Open Group grants you permission to translate its copyrighted material into **<Farsi(persian)>**, for educational purposes, subject to the following terms and conditions :

1. The material for which permission is granted is: "**Open Information Security Management Maturity Model (O-ISM3), Version 2.0**" (the "Standard")
2. Distribution of translation version of the Standard, and any other derivatives, is for educational purposes only. No commercial exploitation of is permitted.
3. The following notice shall be displayed in the front matter and all materials derived from the translated version (whether published or electronic):

   "Translated under permission granted by The Open Group, L.L.C. In the event of any discrepancy between this translated version and the official standard, the official standard found at https://publications.opengroup.org/c17b remains the authoritative version for all purposes. ©The Open Group. All rights reserved."
4. Reproduced graphics or illustration shall be marked © The Open Group.

Please please indicate your acceptance of these terms and conditions by signing this letter where indicated and returning it to me for countersignature. This grant will take effect on the last date signed.

AGREED & ACCEPTED		THE OPEN GROUP, L.L.C.	
Signature		Signature:	
Name:	Mohammad Shervin Jafarzadeh	Name:	
Title:		Title:	VP, Standards & Certification
Email:	Shervin1981@gmail.com	Email	a.josey@opengroup.org
Date :	1st Februry 2022	Date:	1st February 2022

تقدیم به مادرم ،

پدرم ،

و همسرم

که حضورشان در زندگی، دلیل بودنم است

و تقدیم به دخترم ،

گلاریس

استاندارد شرکت Open Group

Open Information Security Management Maturity Model (O-ISM3), Version 2.0
ISBN: 1-937218-98-0

شماره سند C17B:

منتشر شده در سپتامبر ۲۱۰۷، توسط شرکت Open Group

نظرات نسبت به مندرجات این سند را می‌توانید به آدرس زیر:

The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom

یا به پست الکترونیکی زیر ارسال کنید:

ogspecs@opengroup.org

فهرست مطالب

مقدمه اندرو جوزی

قائم مقام شرکت Open Group

(برای خوانندگان فارسی زبان)

استاندارد O-ISM3 که نام خود را از مدل بلوغ مدیریت امنیت اطلاعات مؤسسه Open Group گرفته است، با هدف کمک به مدیران و کارشناسان امنیت اطلاعات برای مدیریت مؤثرتر امنیت اطلاعات منتشر شده است.

O-ISM3 بهبود مستمری را برای مدیریت امنیت اطلاعات به ارمغان می‌آورد و چارچوبی برای تصمیم‌گیری‌های امنیتی ارائه می‌دهد که ماهیت آن رویکرد بالا به پایین است، جایی که کنترل‌های امنیتی، اهداف امنیتی و تصمیم‌گیری‌های مربوط به هزینه‌ها بر اساس اهداف تجاری (و همسو با آن‌ها) هدایت می‌شوند.

O-ISM3:

- ✓ چارچوبی برای همسو کردن اهداف و شاخص‌های کمی امنیتی با اهداف کلی کسب‌وکار فراهم می‌کند
- ✓ یک رویکرد بهبود مستمر موردنیاز را برای مدیریت امنیت اطلاعات ارائه می‌دهد
- ✓ نتایج امنیتی را با عبارات مثبت بیان می‌کند

O-ISM3 را می‌توان به عنوان یک متدولوژی بالا به پایین برای مدیریت کل برنامه امنیت اطلاعات پیاده‌سازی کرد، همچنین می‌توان آن را به صورت تاکتیکی‌تر اجرا و برنامه را تنها با چند فرایند امنیت اطلاعات آغاز کرد.

و بدین ترتیب، می‌تواند برای سازمان‌ها و صنایع گوناگون در اندازه‌های مختلف، امنیت اطلاعات و سطوح بلوغ مختلف و ارزشمندی را ارائه کند.

استاندارد O-ISM3 به صورت رایگان در وب‌سایت The Open Group موجود است (ثبت‌نام الزامی است)، https://www.opengroup.org/library/c17b.

اندرو جوزی

قائم مقام گواهینامه و استانداردهای

مؤسسه Open Group

سخن مترجم

همانطور که امروزه شاهد هستیم با رشد فناوری و رسوخ مدرنیته در زندگی روزمره انسان‌ها، سازمان‌ها وادار به پذیرش تغییر مدل کسب‌وکار خود شدند، چرا که در صورت عدم ورود به دنیای مدرن و با حضور رقبای جدید، محکوم به نابودی خواهند بود، این تغییر که غالباً با آمدن سیستم‌های مکانیزه همراه است، موجب تغییرات کلی و جزیی در سازمان‌ها می‌شود. افزایش سرعت در ارائه خدمات و تعاریف جدید مشتری‌مداری، تنوع در تولید محصولات و افزایش کیفیت خدمات، همه مواردی است که در این تحول، صورت می‌گیرد. طبیعی است که در چنین شرایطی اتکای سازمان‌ها به دانش و جایگاه خود در جامعه بیشتر شده و باعث گردیده نگاه سازمان‌ها علاوه بر حفاظت از دارایی‌های خود از شکل سنتی که بیشتر در قالب حفاظت فیزیکی مطرح بود، به حفظ دارایی‌های اطلاعاتی در فضای سایبری نیز توجه ویژه‌ای داشته باشند.

بی‌شک امروزه امنیت اطلاعات یکی از مهم‌ترین دغدغه‌های سازمان‌هاست. بعضاً شاهد هستیم سازمان‌ها در مدت یکسال هزینه‌های زیادی را صرف موضوع امنیت اطلاعات خود می‌کنند. با خریدهای سیستم‌های امنیتی، تجهیزات نظارتی و کنترلی و دیوارهای آتش، لایسنس‌های ابزارهای امنیتی و ...، با این حال دست آخر سازمان‌ها دچار حملات سایبری شده که کل اعتبار و شهرت یک سازمان را خدشه‌دار می‌سازد. ریشه این اتفاقات آنجاست که سازمان‌ها صرفاً نسبت به تجهیز کردن خرید ابزارهای امنیتی اقدام می‌کنند و از تدوین یک خط‌مشی و نظامنامه امنیت اطلاعات، پیاده‌سازی فرایندها، تعریف اهداف امنیتی هم‌راستا با اهداف کسب‌وکار سازمان غافلند. در سال‌های اخیر به‌واسطه وقوع حوادث امنیتی و تهدیدهای موجود در فضای سایبری، برخی سازمان‌ها نسبت به پیاده‌سازی استاندارد سیستم مدیریت امنیت اطلاعات معروف به ISMS اقدام کردند که گامی مثبت و مؤثر در راستای نظام‌مند کردن فرایندهای امنیتی در یک سازمان، با تعریف خط‌مشی، اهداف و پایش و بازنگری سیستم در بازه‌های زمانی تعریف شده است.

اما باید توجه داشت، استانداردها برای برقراری امنیت اطلاعات در یک سازمان به کمینه اقدامات توجه داشته و همان الزامات خواسته‌شده استاندارد را مورد ممیزی قرار می‌دهند. این اقدام هر چند برای یک سازمان تازه وارد به محیط مدیریت سیستم‌های امنیتی مثبت و مثمرثمر است، اما حال با مرور زمان و طی چند چرخه از استقرار سیستم مدیریت امنیت اطلاعات؛ مدیران، کارکنان دچار خستگی و رخوت شده و بعضاً فرایندها اثربخشی خود را از دست می‌دهند. در اینجاست که سازمان‌ها باید هم‌راستا با اجرای

الزامات استاندارد، قوانین بالاسری و توصیه‌های امنیتی نگاهی به بهبود فرایندها، تفکر فرایندی، رویکرد فرایند داده‌گرا، مدیریت و استخراج نیازمندی‌های سازمان، چرخه حیات توسعه سیستم، مدیریت ارتباطات، مدیریت پروژه‌های فناوری اطلاعات داشته باشد.

فرایندهای ایجاد شده سیستم‌های مدیریتی که در یک سازمان جاری می‌شوند، جزء اصلی تغییرات سازمان در تحولات سازمانی هستند. و بلوغ سازمان یک مفهوم بسیار کاربردی و مهم در مدیریت بهبود فرایند است. بلوغ سازمان نشان می‌دهد ابزارهای اندازه‌گیری و تحلیلی بسیار مناسبی برای اندازه‌گیری اثربخشی فرایندهای سازمانی وجود دارد. ارزیابی بلوغ نه تنها سطح فعلی قابلیت‌ها و جایگاه بلوغ سازمان برای طراحی و اجرای استراتژی را مشخص می‌کند، بلکه حوزه‌هایی را که نقاط ضعف سازمان در این رابطه به شمار می‌آیند نیز تعیین می‌کند. یکی از مهم‌ترین معیارهای پیشرفت کسب‌وکار یک سازمان، بلوغ آن است و داشتن اطلاعات در خصوص داشتن میزان بلوغ سازمان ضروری است.

برای این منظور، نیاز به یک معیار خوب جهت اندازه‌گیری بلوغ است. معیاری که امکان مقایسه دقیق با سازمان‌های رقیب، شرکای استراتژیک یا حتی مشتریان را فراهم کند.

از آنجا که سیستم مدیریت امنیت اطلاعات، از اهمیت بالایی برای سازمان‌ها برخوردار است لذا محاسبه میزان بلوغ سازمان در این حوزه ضرروت داشته و نشان‌دهنده مسیر حرکت سازمان در اجرای موفق و اثربخش فرایندها، بهبود و افزایش کارایی فرایندها و نزدیکی اهداف امنیت به اهداف سازمان خواهد بود.

مؤسسه Open Group کنسرسیومی جهانی است که امکان دستیابی به اهداف کسب‌وکار را از طریق تولید و نگارش استانداردهای فناوری اطلاعات فراهم می‌کند. در سال ۲۰۱۷ مدلی را برای محاسبه بلوغ سیستم مدیریت امنیت اطلاعات در سازمان‌ها تحت عنوان O-ISM3 ارائه کرده است. کتاب حاضر ترجمه کامل متن O-ISM3 است که در اختیار خوانندگان محترم قرار گرفته است.

کتاب پیش‌رو برای تمامی مدیران ارشد سازمان‌ها، مدیران فناوری اطلاعات، مدیران امنیت اطلاعات، کارشناسان فناوری اطلاعات، کارشناسان امنیت اطلاعات و ممیزان و بازرسان سیستم‌های امنیت اطلاعات مفید بوده و می‌تواند به عنوان الگویی برای رتبه‌بندی سازمان‌ها در رسیدن به نقطه‌ای مطلوب در مدیریت امنیت اطلاعات مرجع واقع شود.

محمد شروین جعفرزاده

تهران - فروردین ۱۴۰۱

پیشگفتار

شرکت Open Group

شرکت Open Group کنسرسیومی جهانی است که امکان دستیابی به اهداف کسب‌وکار را از طریق استانداردهای فناوری اطلاعات فراهم می‌کند. این شرکت با بیش از ۵۰۰ سازمان عضو دارای تنوع بالایی در عضویت است که همه بخش‌های جامعه فناوری اطلاعات شامل مشتریان، تأمین‌کنندگان سیستم‌ها و راه‌حل‌ها، فروشندگان ابزارها، انسجام‌دهندگان و مشاوران و همچنین دانشگاهیان و پژوهشگران را فرامی‌گیرد. هدف از طیف عضویت در شرکت Open Group عبارت است از:

- ✓ جمع‌آوری، ادراک و برطرف کردن الزامات کنونی و نوظهور، ایجاد خط‌مشی‌ها و به اشتراک گذاشتن به‌روش‌ها[1]
- ✓ تسهیل تعامل‌پذیری، ایجاد اجماع و تکامل و یکپارچه‌سازی مشخصات و فناوری‌های متن‌باز[2]
- ✓ خدمات صدور گواهینامه‌های برتر در صنعت[3]، اطلاعات بیشتر درباره این شرکت در وب‌سایت www.opengroup.org در دسترس است.

شرکت Open Group طیف وسیعی از اسناد فنی را منتشر می‌کند که بیشتر آن‌ها به توسعه استانداردها و راهنماهای Open Group[4] می‌پردازند که شامل گزارش‌های رسمی[5] (دولتی)، مطالعات فنی، اسناد گواهی و آزمون و عناوین کسب‌وکار نیز هستند. جزئیات کامل و کاتالوگ در وب‌سایت www.opengroup.org/bookstore قرار دارند.

خوانندگان باید توجه کنند که هر سند منتشر شده ممکن است به شکل اصلاحیه[6] به‌روزرسانی شود.

1- Best Practises
2- Open Source
3- Premier Certification Service
4- Open Group Standards and Guides
5- White Papers
6- Corrigenda

سند حاضر

این سند استاندارد شرکت Open Group برای مدل باز بلوغ مدیریت امنیت اطلاعات است. سند مذکور توسط شرکت Open Group تهیه و تصویب شده است.

O-ISM3 چارچوب Open Group برای مدیریت امنیت اطلاعات و در عین حال، چارچوب مدیریت اطلاعات در زمینه‌ای وسیع هستند. هدف از این استاندارد حصول اطمینان از اجرای فرایندهای امنیت در هر سازمانی است، به‌گونه‌ای که استاندارد مذکور در سطحی سازگار با الزامات کسب‌وکاری آن سازمان عمل کند. استاندارد O-ISM3 عاری از فناوری است. این استاندارد تعداد جامع و متناسبی از فرایندهای امنیت اطلاعات را تعریف می‌کند که برای نیازهای بیشتر سازمان‌ها کفایت می‌کنند؛ در این استاندارد کنترل(های) مرتبط با امنیت در هر فرایند به‌منزله زیرمجموعه اصلی آن شناسایی می‌شوند. استاندارد O-ISM3 از این جهت به‌طور کامل با استانداردهای باسابقه ISO/IEC 27000:2009، COBIT® و ITIL® در این حوزه‌ها سازگار است. به‌علاوه، O-ISM3 علاوه بر تکمیل چارچوب TOGAF® برای معماری سازمان، معیارهای عملیاتی و تغییرات مجاز آن‌ها را نیز تعریف می‌کند.

تقاضا، عامل پیشران تمام سیستم‌های کارآمد کسب‌وکار است؛ همه سیستم‌های مذکور از اندازه‌گیری شاخص‌ها برای بهبود کیفیت استفاده می‌کنند. استاندارد O-ISM3 برای ساخت، متناسب‌سازی و بهره‌برداری از سیستم مدیریت امنیت اطلاعات[1] چارچوبی را فراهم می‌کند. استفاده از این معیارها تضمین می‌کند که این سیستم مدیریت از معیارهای عینی و کمّی برای تأثیر بر تصمیم‌های کسب‌وکاری، درباره تخصیص اثربخش منابع به سیستم مدیریت امنیت فناوری اطلاعات و پاسخ به تغییرات استفاده می‌کند. بهترین و سودمندترین دستاورد برای امنیت اطلاعات ریسک کمتر و بازگشت سرمایه[2] بیشتر است.

کارایی فرایندهای امنیت اطلاعات هر سازمان در گرو مستندسازی، اندازه‌گیری و مدیریت هستند. استاندارد O-ISM3 بلوغ را برحسب عملکرد فرایندهای کلیدی امنیت تعریف می‌کند. در این سیستم، قابلیت[3] برحسب معیارها و رویه‌های مدیریتی[4] معمول تعریف می‌شود. پیاده‌سازی O-ISM3 مستلزم آن است که اهداف و اهداف کمّی امنیت از اهداف کسب‌وکار اخذ شوند و اندازه‌گیری‌های رسمی اثربخشی هر فرایند مدیریت امنیت صورت پذیرد.

1- Information Security Management System (ISMS)
2- Return on Investment (ROI)
3- Capability
4- Management Practices

سازمان‌ها در بخش‌های مختلف کسب‌وکار و در کشورهای مختلف الزامات کسب‌وکاری و تاب‌آوری‌های مختلفی در ریسک[1] دارند. چارچوب O-ISM3 به مدیران امنیت اطلاعات در ارزیابی محیط عملیاتی آن‌ها و طرح‌ریزی فرایندهای مدیریت امنیت کمک می‌کند، بنابراین فرایندهای مذکور ضمن مقرون‌به‌صرفه بودن با اهداف کسب‌وکاری سازمان‌های خود نیز سازگار خواهند بود.

1- Risk Tolerances

علائم تجاری

The Open ،OpenPegasus® ،Making Standards Work® ،DirecNet® ،ArchiMate® Open Brand X® و نشان X/Open® ،UNIXWARE® ، UNIX®،TOGAF® ،Group® علائم تجاری ثبت‌شده هستند و Boundaryless Information Flow™، Build with Integrity Buy with Confidence™، Dependability Through Assuredness™، EMMM™، FACE™ نشان FACE™، IT4IT™ نشان IT4IT™، O-DEF™، O-PAS™، Open Open Trusted ،Open Process Automation™ ،Open Platform 3.0™ ،FAIR™ Open و نشان Open O™ نشان SOSA™، Platform 3.0™، Technology Provider™ Group Certification (Open O و check™) علائم تجاری شرکت Open Group هستند.

CMMI® و P-CMM® علائم تجاری مؤسسه CMMI Institute LLC هستند.

COBIT® علامت تجاری ثبت‌شده انجمن Information System Audit and Control Association (ISACA) است.

ITIL® علامت تجاری شرکت AXELOS Limited است.

Microsoft® و Windows® علائم تجاری شرکت Microsoft Corporation مستقر در ایالات‌متحده و سایر کشورها هستند.

همه دیگر نام‌های تجاری، شرکت‌ها و اسامی محصولات تنها به‌قصد شناسایی استفاده شده‌اند و ممکن است علائم تجاری باشند که جز دارایی مالکانشان به حساب می‌آیند.

سپاسگزاری

شرکت Open Group مراتب سپاسگزاری خود را از آنانی که با فعالیت، سازمان یا نظرات ارزشمند خود به تهیه این استاندارد O-ISM3 کمک کردند اعلام می‌دارد:

مؤلف اصلی (همه نسخه‌ها)

- Vicente Aceituno از کنسرسیوم ISM3

یاریگران کنسرسیوم ISM3 تا زمان تهیه نسخه فوریه ۲۰۱۱ که از سوی شرکت Open Group منتشر شده است:

- Chris Carlson از شرکت بوئینگ
- Anton Chuvakin از شرکت Security Warrior Consulting
- Ian Dobson از شرکت Open Group
- Phil Griffin از شرکت Griffin Consulting
- Jim Hietala از شرکت Open Group
- Alex Hutton از شرکت Verizon
- Francois Jan از شرکت Arismore
- Mike Jerbic از شرکت Trusted Systems Consulting Group
- Mary Ann Mezzapelle از شرکت HP
- Edward Stansfeld از شرکت Audit Scotland

صمیمانه از نویسندگان برجسته برای تهیه نسخه‌هایی (تا نسخه v2.30) تشکر می‌شود که از سوی کنسرسیوم ISM3 منتشر شدند:

- Alex Hutton از شرکت Riskana1ys.is
- Robert Kloots از شرکت CSF bv
- Anup Narayanan از شرکت First Legion Consulting
- Anthony B. Nelson از شرکت Estec Security

- Kelly Ray از شرکت Open Compliance and Ethics Group
- Arthur Richard از شرکت Kuwait Oil Company
- George Spafford از شرکت Pepperweed Consulting
- Edward Stansfeld، سردبیر و داور اصلی و نویسنده از شرکت Audit Scotland
- K Rama Subramaniam از شرکت Valiant Technologies Pvt Ltd
- Shane Wansink از دانشگاه Deakin
- Jeff Warren از اداره DHS دولت ویکتوریا/استرالیا

اسناد مرجع

توجه داشته باشید که لینک‌های زیر به زمان نگارش این سند مربوط می‌شوند و اطمینانی به صحت آن‌ها در آینده وجود ندارد.

پارادایم‌ها

در این استاندارد به پارادایم‌های زیر استناد می‌شود.

- Defense in Depth
- Keep it Simple, Stupid
- Mayfield’s Paradox
- Minimum Privilege
- Need to Know
- Objective-Value-Activity
- People, Process, and Technology
- Prevention, Detection, and Response
- Security by Design
- Shewhart Cycle or Deming Wheel (Plan, Do, Check, Act)

اسناد

در این استاندارد به اسناد ذیل استناد می‌شود.

- AS 5037:2005: Knowledge Management – A Guide; refer to: www.itgovernance.co.uk
- AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines, Joint Australia/New Zealand adoption of ISO 31000:2009 (supersedes

AS/NZS 4360:2004); refer to: www.standards.govt.nz/search-and-buy-standards/standards-information/risk-managment
- Building Security In Maturity Model (BSIMM); refer to: www.bsimm.com
- BS 25999: Business Continuity Management (BCM); refer to: https://en.wikipedia.org/wiki/BS_25999
- Capability Maturity Model Integration (CMMI®), CMMI Institute; refer to: http://cmmiinstitute.com
- Center for Internet Security (CIS); refer to: www.cisecurity.org
- CLUSIF MEHARI; refer to: https://clusif.fr/home-page-english
- COBIT®: Framework for IT Governance and Control, ISACA; refer to: www.isaca.org/knowledge-center/cobit/pages/overview.aspx
- CRAMM (CCTA Risk Analysis and Management Method); refer to: https://en.wikipedia.org/wiki/CRAMM
- EBIOS: Expression of Needs and Identification of Security Objectives; refer to: www.ssi.gouv.fr/archive/en/confidence/ebiospresentation.html
- Open Enterprise Security Architecture (O-ESA), Open Group Guide (G112), April 2011, published by The Open Group; refer to: www.opengroup.org/bookstore/catalogg112.htm
- Federal Enterprise Architecture (FEA); refer to: https://en.wikipedia.org/wiki/Federal_enterprise_architecture
- HIMIS (Human Impact Management for Information Security); refer to: http://himis.s3.amazonaws.com/himis.pdf
- IETF RFC 3768: Virtual Router Redundancy Protocol (VRRP), 2004; refer to: www.ietf.org/rfc/rfc3768.txt
- Information Security Governance: Towards a Framework for Action, Business Software Alliance, 2003; refer to: www.entrust.com/wp-content/uploads/2013/05/ITgovtaskforce.pdf
- Institute for Security and Open Methodologies (ISECOM) Open Source Security Testing Methodology Manual (OSSTMM); refer to: www.isecom.org/osstmm
- ISACA: IS Audit and Assurance Standards; refer to: www.isaca.org/knowledge-center/standards/pages/default.aspx
- ISACA: IS Control Professionals Standards, in IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals; refer to: www.isaca.org/knowledge-center/standards/documents/it-audit-assurance-guidance-1march2010.pdf
- $(ISC)^2$ CISSP; refer to: www.isc2.org
- ISO 9000:2005: Quality Management Systems – Fundamentals and Vocabulary; refer to: www.iso.org/standard/42180.html
- ISO 9001:2000: Quality Management Systems – Requirements; refer to: www.iso.org/standard/21823.html

- ISO 15228: 2005: Textile Machinery and Accessories – Profile Reeds for Air Jet Weaving Machines – Dimensions; refer to: www.iso.org/standard/26973.html
- ISO 15489:2001: Information and Documentation – Records Management; refer to: www.iso.org/standard/62542.html
- ISO/IEC 12207:2008: Systems and Software Engineering – Software Lifecycle Processes; refer to: www.iso.org/standard/43447.html
- ISO/IEC 15408:2009: Information Technology – Security Techniques – Evaluation Criteria for IT Security; refer to: www.iso.org/standard/50341.html
- ISO/IEC 21827:2008: Information Technology – Security Techniques – Systems Security Engineering – Capability Maturity Model (SSE-CMM); refer to: www.iso.org/standard/44716.html
- ISO/IEC 24762:2008: Information Technology – Security Techniques – Guidelines for Information and Communications Technology Disaster Recovery Services; refer to: www.iso.org/standard/41532.html
- ISO/IEC 27000:2009: Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary; refer to: www.iso.org/standard/41933.html
- ISO/IEC 27001:2005: Information Technology – Security Techniques – Information Security Management Systems – Requirements; refer to: www.iso.org/standard/42103.html
- ISO/IEC 27002:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management; refer to: www.iso.org/standard/50297.html
- ISO/IEC 27004:2009: Information Technology – Security Techniques – Information Security Management – Measurement; refer to: www.iso.org/standard/42106.html
- ISO/IEC 27005:2008: Information Technology – Security Techniques – Information Security Risk Management; refer to: www.iso.org/standard/42107.html
- ISO/IEC TR 18044:2004: Information Technology – Security Techniques – Information Security Incident Management; refer to: www.iso.org/standard/35396.html
- IT Infrastructure Library (ITIL®) IT Service Management (ITSM); refer to: www.itil-itsm-world.com
- Joint Publication (JP) 3-13: Information Operations, 2006; refer to: www.information-retrieval.info/docs/jp3_13.pdf
- Joint Publication (JP) 3-13.3: Operations Security, 2012; refer to: https://publicintelligence.net/jcs-opsec
- Joint Publication (JP) 3-13.4 (formerly JP 3-58): Military Deception, 2006; refer to: www.information-retrieval.info/docs/jp3_13_4.pdf
- MAP MAGERIT; refer to: www.csi.map.es/csi/pg5m20.htm

- National Security Agency (NSA); refer to: www.nsa.gov
- NIST Cybersecurity Framework (CSF); refer to: www.nist.gov/cyberframework
- NIST Role-Based Access Control (RBAC); refer to: http://csrc.nist.gov/groups/SNS/rbac
- NIST Special Publication (SP) 800-30: Guide for Conducting Risk Assessments, September 2012; refer to: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- NIST Special Publication (SP) 800-55: Performance Measurement Guide for Information Security, July 2008; refer to: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf
- OASIS Reference Model for SOA; refer to: www.oasis-open.org
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), CERT; refer to: www.cert.org/octave
- OWASP (Open Web Application Security Project); refer to: www.owasp.org
- People Capability Maturity Model® (P-CMM®), CMMI Institute; refer to: http://cmmiinstitute.com
- پروژه Quant, Securosis; refer to: https://securosis.com/projectquant
- Risk Taxonomy (O-RT), Version 2.0, an Open Group Standard (C13K), October 2013, published by The Open Group; refer to: www.opengroup.org/bookstore/catalog/c13k.htm
- SABSA (Sherwood Applied Business Security Architecture); refer to: www.sabsa-institute.org
- SANS; refer to: www.sans.org
- Serenity Project (EU); refer to: http://eu-serenity.sourceforge.net
- Six Sigma DMAIC (Define, Measure, Analyze, Improve, Control) Roadmap; refer to: www.isixsigma.com/new-to-six-sigma/dmaic/six-sigma-dmaic-roadmap
- SPSMM (Secure Programming Standards Methodology Manual); refer to: www.isecom.org/research/spsmm.html
- Standardized Information Gathering, BITS; refer to: www.sharedassessments.org
- Statement on Auditing Standards (SAS) No. 70; refer to: sas70.com
- Systems Security Engineering Capability Maturity Model (SSE-CMM); refer to: www.sse-cmm.org
- TOGAF® 9.1, an Open Group Standard (G116), December 2011, published by The Open Group; refer to: www.opengroup.org/bookstore/catalog/g116.htm
- The Survivability of Network Systems: An Empirical Analysis, Technical Report, Carnegie Mellon University, Software Engineering Institute, 2000; refer to: ftp://ftp.sei.cmu.edu/pub/documents/00.reports/pdf/00tr021.pdf

برخی از مراجع ذیل ایده‌های ارزشمندی برای تهیه این استاندارد (O-ISM3) ارائه کرده‌اند، بنابراین در اینجا از آن‌ها به‌مثابه منابع مؤثر قدردانی می‌شود، اگرچه ممکن است به‌طور مستقیم به همه آن‌ها ارجاع داده نشده باشد.

- American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP); refer to: www.aicpa.org
- Balanced Scorecard; refer to: https://en.wikipedia.org/wiki/Balanced_scorecard
- Business Process Improvement; refer to: https://en.wikipedia.org/wiki/Business_process_management
- Certified Information Systems Auditor (CISA), ISACA; refer to: www.isaca.org
- Certified Information Security Manager (CISM), ISACA; refer to: www.isaca.org
- Corporate Information Security Working Group (CISWG) Report of the Best Practices and Metrics Teams, 2004; refer to: www.educause.edu/ir/library/pdf/CSD3661.pdf
- Designing Secure Information Systems and Software: Critical Evaluation of the Existing Approaches and a New Paradigm, Mikko Siponen, 2002; refer to: http://herkules.oulu.fi/isbn9514267907/isbn9514267907.pdf
- EA 7/03: EA Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems; refer to: www.european-accreditation.org
- Events Logging Markup Language (ELML); refer to: www.ISM3.com
- Federal Information Security Management Act (USA), 2002; refer to: https://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002
- IETF RFC 2119: Key Words for Use in RFCs to Indicate Requirement Levels; refer to: www.ietf.org/rfc/rfc2119.txt
- Information Assurance Markup Language (IAML); refer to: www.ISM3.com
- Information System Security Association (ISSA) Generally Accepted Information Security Principles (GAISP); refer to: www.issa.org
- ISO 19011:2002: Guidelines for Quality and/or Environmental Management Systems Auditing; refer to: https://www.iso.org/standard/31169.html
- Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security, University of New Haven, 2000; refer to: https://hackerfall.com/story/mayfields-paradox-a-fundamental-principle-of-infor
- NIST SP 800-53: Security Controls and Assessment Procedures for Federal Information Systems and Organizations; refer to: https://nvd.nist.gov/800-53/Rev4
- OCEG Measurement & Metrics Guide; refer to: www.oceg.org/view/mmg

- Shewhart-Deming Control Charts; refer to: https://en.wikipedia.org/wiki/Control_chart
- Towards Maturity of Information Maturity Criteria: Six Lessons Learned from Software Quality Criteria, Mikko Siponen, 2002; refer to: https://pdfs.semanticscholar.org/bd2c/076ec249cf35917f0cb78bd5f822dc683414.pdf